Research and Documentation Centre

Cahier 2023-12a

Police Hacking regulation abroad

A comparative law study into legal regulations and safeguards regarding the quality of data

Research and knowledge centre for
the Ministry of Justice and Security

Cahier 2023-12a

Police Hacking regulation abroad

A comparative law study into legal regulations and safeguards regarding the quality of data

J.J. van Berkel
A. van Uden
J.H. Goes

Cahier
This series comprises overviews of studies carried out by or for the WODC Research and Documentation Centre. Inclusion in the series does not mean that the sheet's contents reflect the viewpoint of the Minister of Justice.

Table of contents

Summary

The Dutch Computer Crime Act III (CCIII) came into effect on 1 March 2019. Among other things, this Act introduces the power of the police to carry out hacking operations. The new Sections 126nba, 126uba, 126zpa in the Code of Criminal Procedure will allow specially authorised investigating officers to covertly and remotely intrude into computer systems under certain conditions and investigate them. The police can carry out investigative actions using technical tools. In principle, a technical device must be inspected and approved by an independent Dutch National Examination Service (*de Keuringsdienst*) prior to its use, in order to guarantee the reliability, traceability and integrity of the evidence.

The Justice & Security Inspectorate (hereinafter Inspectorate) supervises the implementation of the hacking power. In its first Report in 2020, it concluded that the use of technical tools for hacking powers and the examination of these tools were not yet proceeding as intended under the legal framework. In his response to the first Inspectorate Report, the then Minister of Justice and Security indicated that he would have an investigation into the safeguards of technical tools used by foreign police authorities. The present report is the result of this research. This report also supplements the previously published evaluation of the use of the hacking power in the Netherlands, carried out by the WODC.

Research question

The central research question for this study is as follows:

What safeguards govern hacking powers abroad, more specifically the use of technical tools, and how does this compare with the Dutch situation?

The central research question is answered on the basis of the following subquestions:

1 What countries allow 'authorised hacking' and on the basis of which legal ground can foreign police services carry out hacking operations in their own country?
2 What statutory conditions apply in other countries for police services to deploy the hacking power?
3 To what extent do other countries examine technical tools and what has been laid down in legislation and regulations on this?
4 To what extent are there any other rules to ensure the reliability, traceability and integrity of data obtained with the use of technical tools?
5 How does the working method abroad compare with the Dutch working method regarding the approval of technical tools and any other safeguards to achieve data reliability, integrity and traceability?

Methods of research

We first made a broad inventory to map out which countries have legal hacking powers. To be able to speak of a hacking power, we assumed that the hacking power is carried out secretly and remotely. As part of the broad inventory, virtually all European countries were examined, with the addition of the United States, Canada and

Australia. Based on the broad inventory, a selection was made of five countries that were studied in more detail: Belgium, Germany, France, Sweden and Switzerland. Various research methods were used to answer the research questions: document study (laws and regulations and relevant (grey) literature), written questionnaires and interviews.

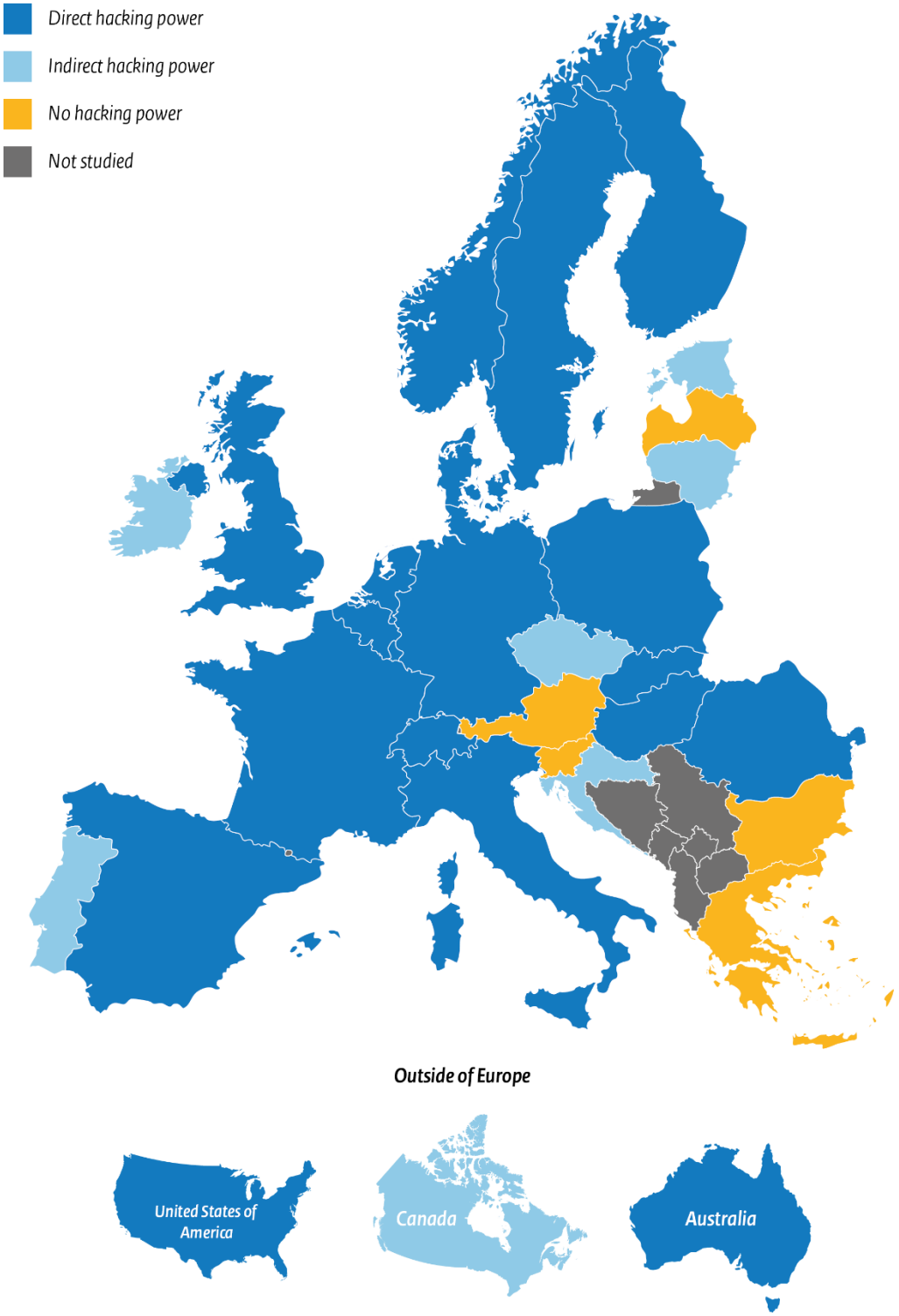
Broad inventory

Based on the broad inventory, a number of topics are discussed in this report. In this summary, attention is paid to the presence of a hacking power, the examination of technical resources and the presence of an inspection body, the guarantees for documentation, storage and judicial supervision, and the notification obligation and the right of inspection.

Presence of hacking power

The figure on the next page features a map of all the countries included in this study. The figure indicates whether a country has set up a statutory power of the police to carry out hacking operations, and if so, whether this is a direct or indirect power. A direct power applies if the law explicitly refers to the possibility of covertly and remotely intruding into a computer system and undertaking one or more investigative actions within that system. An indirect power applies if the hacking power forms part of a general provision. Consider, for example, the power to intercept telecommunications, whereby the law text does not specifically mention the hacking power, though the power could be used for that purpose.

Country overview – hacking power



The maps are adaptations of works by Maix (Europe; CC BY-SA 3.0), Theshibboleth/Lokal_Profil (VS; CC BY-SA 2.5), Paul Robinson/Lokal_Profil (Canada; public domain) and Rycherr (Australia; CC BY-SA 4.0 and previous versions).

Examination of technical tools and supervisory body

None of the countries has established an independent body in charge of examining the technical tools before they are deployed based on a comprehensive examination protocol. Some countries do have a testing procedure, however, these procedures are not performed by an independent examination body. Furthermore, for those other countries that do have an examination or testing procedure, it is unknown what the procedure consists of. Germany constitutes an exception in this regard. Even in that country, it is not entirely clear what the examination entails, but it is clear that it is based on an SLB guideline specifically designed for it. See Section 4.8.

In other countries, the supervision of hacking operations by an independent body is limited, thereby not including the trial court. Australia, Denmark, Norway, the UK and Sweden have independent bodies performing some level of supervision of the execution of the hacking power. Owing to its technical expertise, Germany has an authority that advises on the deployment and development of technical tools. France has a specific authority responsible for the design, supervision and implementation of technical tools used for hacking operations.

Safeguards regarding documentation, storage and judicial supervision

Almost all countries require some sort of documentation with regard to documenting and logging operative actions. As a minimum, they require an official report documenting all actions. Some countries take it a step further and require the logging of all actions. During our research, it remained unclear to what extent five countries have requirements to document and register operative actions.

There is judicial supervision in Belgium, France, Croatia, Portugal and Spain *during* the deployment of the hacking power. This means the police must provide interim updates on progress to the judge who issued the order. In some cases, the judge may withdraw the authorisation for the hacking operations based on those status updates. As far as we know, there is no interim judicial review in the remaining countries.

Twenty countries have included safeguards in their laws regarding the storage of data collected with the use of hacking powers. These safeguards include the sealed storage of data or the storage of data in a secure environment. In the case of the remaining countries, nothing is included in the law or it has not become clear to us whether countries have set formal or informal safeguards.

Trial and right to inspection

Thirteen countries have included a notification obligation in the law. This means that those persons whose computer system was hacked must be informed within a predefined term that this hacking power had been deployed. In half of these countries, notification can be deferred or sometimes even omitted if the interests of the investigation may be compromised. In nearly all countries, the suspect will be notified if the case is brought before the court. Seventeen countries have explicitly included the right to inspect obtained data in legislation. In many cases, the defence may receive a copy of the data obtained. Among the remaining countries, our inventory did

not show whether this hacking power is covered by a specific legal provision regarding the right to inspection.

In-depth country comparison

A number of countries have been studied in more depth. These countries have been compared with each other and with the Netherlands. Therefore we first describe the most important bottlenecks in the Netherlands. Then follows the country comparison.

Main issues and bottlenecks in examining technical tools in the Netherlands

For the introduction of the hacking power, the Dutch legislator opted to follow the examination system of technical tools already set in place for existing (special) investigative powers. A separate decision was prepared for the authorised hacking titled 'the Decision on intruding into automated information systems (hacking)', hereinafter: the Decision. The Decision sets a number of requirements for technical tools, including requirements aimed at integrity, traceability and reliability of the data collected, hereinafter: quality. The Dutch National Examination Service is tasked with examining the tools in the Netherlands, thereby applying an examination protocol based on various articles from the Decision. In principle, the police must make use of technical tools that have been examined and approved prior to their use. This is subject to a number of exceptions: 1) a technical tool may be examined afterwards, 2) it is possible to switch to manual deployment or 3) the public prosecutor decides that the tool cannot be examined 'on account of its nature'.

The Reports from the Inspectorate of Justice and Security and the first evaluation report from the Research and Documentation Centre show that the examination and the use of technical tools do not always proceed as intended by law. Pre-approved technical tools are hardly ever deployed, and the examination is a major bottleneck for investigation practices. Different aspects play a role here:

- The turnaround time of an examination takes a relatively long time, at least four months. That timeframe does not always match the promptness that may be required within an investigation.
- Adjusting a technical tool that has not been approved always requires a new examination and thus takes time.
- The Decision demands, and consequently so does the Dutch National Examination Service that technical tools must meet all requirements for the technical tool to be approved. Investigation practices, however, question the usefulness and necessity of all requirements and the compliance thereof.
- The deployment of technical tools takes place in an environment which Digit, the police team executing the power, cannot always control. For example, Digit cannot exercise any influence over what suspects do with their computer systems. Any action from the owner of the computer system can affect the quality of the data collected. Digit would prefer to focus more on making risk analyses with regard to the technical tool used and the evidential value of the data collected.
- A risk analysis focuses on the risk of data quality being compromised if a technical tool is used that does not meet all requirements.
- Another consideration is the impact of using a technical tool that does not meet all requirements on the evidential value of the data collected. Especially, if the data only form part of the evidence collected.

The majority of police investigations in which hacking operations are carried out make use of a commercial product. Here, too, no pre-approved tools were used. In fact, the products were never submitted for examination, because the Digit public prosecutor decided that the nature of the tools preclude an examination. In so doing, the public prosecutor makes use of the Decision's ground for exception. Incidentally, these products can indeed not be approved under the current examination regime. There are a number of factors that make a commercial tool inherently impossible to approve and/or never to be approved:

- Commercial tools are updated relatively often. The question then becomes, which version or versions should the Dutch National Examination Service approve? If all the versions need to be approved, it would exceed the usual lead time needed for examination and approval in relation to the timeframe within which the police action must take place.
- Operation of these types of tools is a 'black box' for the users, which is why the Dutch National Examination Service is not given access to the exact operation and can therefore not carry out a full examination.
- Suppliers want to have access to their product at all times, to do things like perform maintenance, for example. As a result, the Dutch National Examination Service is not given exclusive access to the tool, which it requires for its examination. Not having exclusive access means no approval, as it cannot be ruled out that a party other than the suspect and the police had access to the data collected. This means that the reliability and integrity of the data cannot be fully guaranteed.

Failing to perform the examination means that a majority of criminal investigations do not comply with a key safeguard with regard to the quality of the data collected. It should be noted, however, that additional technical and tactical safeguards are put in place in this situation to ensure the reliability of the evidence. These tactical safeguards are not included in the examination.

Comparison between countries

In our study, five countries have been studied in more depth: Belgium, Germany, France, Sweden and Switzerland. To compare the countries, a distinction has been made between three phases with regard to the safeguards during the deployment of the hacking power: the phase prior to deployment, during deployment and after deployment of the hacking power.

Safeguards prior to the deployment of the power

Except for Sweden, all countries have some form of examination or testing of the technical tool to be used. However, the manner differs per country. The Netherlands has the most detailed described examination of technical tools. The manner in which Germany has described the criteria appears closest to the way the Netherlands has done this. The German examination is based on the SLB Guideline, which highlights the following themes: protection targets and security measures, work processes and procedures, suppliers, and test policy. Application of the guideline serves as a guiding principle; it is not a legal requirement. A risk analysis is used to identify which objects, e.g. system components such as hardware and software, applications, organisational or personnel issues, pose a risk for these themes. The results of this risk analysis, the determination of the protection needs and the resulting consequences and

implementation thereof are laid down in an IT security concept. Both software suppliers and users of the software must conform to this concept. It is not known what criteria comprise the examinations in the other countries.

The Dutch National Examination Service carries out the examination in the Netherlands. The Dutch National Examination Service is an independent body, though it formally falls under the same organisational unit of the National Police Board to which the team carrying out the hacking operation belongs. In France, the testing is done by a specific government body called STNCJ. This government body is also responsible for the execution of the hacking power. In both countries, the way in which the tasks are assigned may raise the question of how independent the examination is. This applies in particular to France, where it is actually the same organization that carries out the power and inspects the tools. The other countries have the police doing their own testing. It is interesting to note that both in France and Switzerland, the 'examiner' and the 'performing party' are one and the same party. These countries do not consider this to be problematic and proceed on the assumption that the parties act in a fundamentally trustworthy manner. As far as known, there is no formal examination in Sweden. However, they often use standardised software at a later stage of the hacking process, i.e. once the data are placed on the police's systems. This standardised software, for example, involves software that has been certified by other police services such as the Dutch police.

Safeguards during the deployment of the hacking power

The safeguards that must be in place during deployment of the hacking power differ per country. Common safeguards at this stage are forms of logging, reporting, the use of a secured transport of data from the computer system and the storage of data in a secured environment.

There is judicial review in Belgium and France during the hacking operations. The judge granting authorisation for the deployment of the hacking power also supervises the execution thereof. If the execution of the hacking power does not take place in accordance with the conditions of the authorisation, the hacking operations may be terminated. It should be noted in this respect that the judge relies on the information that the police or the public prosecutor provides or may provide during the deployment. The question is thus whether this judicial oversight will actually ensure that a deployment can be terminated mid-term. The judicial oversight in these countries goes beyond the role of the Examining Magistrate in the Netherlands, who principally only oversees the hacking power prior to a deployment or its extension. However, the Netherlands still has the supervision by the Inspectorate of Justice and Security.

Safeguards after the deployment of the hacking power

The most common safeguards pertain to the notification of the deployment of the hacking power to the suspects or the data subjects, the substance of the case at the hearing and the suspect's right to inspection. Notification is not a guarantee in all countries, given that such notification may be omitted if it could compromise ongoing interests of the investigation. The law in Belgium always requires notification. France is the only country in which a suspect does not need to be notified. It goes without saying that if the data hacked form part of the evidence, the suspect is indirectly notified by the inspection of the file. Not all countries have made it clear what

information is included in the file, and to what extent the right to inspection extends. However, it does emerge that in most cases the defence receives a copy of the data collected by means of hacking operations or a collection thereof.

Based on information conveyed in interviews there is still little case law available that calls into question the quality of the data collected by means of hacking operations. This makes it difficult to answer the question of how extensively a session judge assesses the deployment and the data quality. The case law that is available mostly deals with cases where evidence is used based on data from the Encrochat communications service. The French authorities have been able to intercept these communications. Many countries have used Encrochat data as evidence. However, the main issue in these cases was whether this was legally obtained evidence rather than the quality of the data collected. As far as known, the quality of data has only been called into question in Sweden and France. In Sweden, the court dismissed relatively easily the objections raised regarding data quality. The court added that the data, in conjunction with other investigation data, show that 'the messages correspond well to the reality in terms of time and content'. More striking is an October 2022 ruling from France. In this ruling, the court concluded that in the absence of a certificate of truthfulness, it cannot be accepted that nothing is shared about how the evidence was obtained. However, this only applies if the collected data is encrypted. It is likely that the police use the authority to view decrypted messages (live). Therefore, in these cases a certificate is not required.

Another striking issue in terms of the safeguards at the end of deployment is the legal provision applicable in Switzerland that stipulates that it must be made possible to check the source code of the technical tool if so requested by the court. Prior to deployment, it must also be ensured that the supplier cannot access the data. Source code disclosure and access restriction stand out because both issues are a major obstacle in the Netherlands to examining and approving commercial tools. A relevant question, which unfortunately cannot be answered based on our research, is thus to what extent both requirements can ultimately be enforced in Switzerland.

Finally, it is worth noting that Sweden is the only one of five countries that has a specific supervisory body (SIN) that monitors the hacking power. SIN's role in relation to the use of technical tools for the hacking power is still evolving. For the time being, supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness. However, SIN also has the authority to check the technical tools themselves. While SIN's rulings are not binding, authorities generally follow SIN's rulings. SIN has partly similar tasks to the Inspectorate in the Netherlands, but it additionally oversees the lawfulness of the entire process and thus also the activities of both the police and the public prosecutor. SIN can furthermore issue public statements in individual cases. The suspect may also personally request this.

Scenario's

Based on our research, we have formulated three scenarios which could potentially complement the way in which the Netherlands deals with technical tools and data collected by means of the hacking power. These scenarios are described in the text below.

Scenario 1: Source code and monitoring data access

Our research shows that it is required by law in Switzerland that it must be made possible to check the source code of the technical tool if so requested by the court. It must also be ensured that suppliers cannot access the data when these are being collected. These issues specifically form an obstacle in the Netherlands in examining commercially technical tools. It has not become clear to what extent the Swiss authorities have actually been able to fulfil both requirements. As far as is known, there has not yet been a case in which the source code was actually requested. In principle, suppliers do not benefit from giving access to their source codes. The software's working method is a well-kept secret. However, if Switzerland has succeeded in finding a workable solution, it is worth considering whether the police, public prosecutors and policymakers in the Netherlands can also achieve this in a similar manner. This could resolve two major bottlenecks in the examination procedure in the Netherlands.

Scenario 2: Changing supervisory role

During the Dutch legislative process, supervision during the exercise of the power has been an important point of discussion. Extra supervision would be necessary because judges would not always be able to properly assess the evidence collected. It was also expected that a (large) portion of the cases would never be trialled by a court. It has been suggested to set up a body comparable to the Supervisory Committee of the Intelligence and Security Services (CTIVD). Over the years, various authors have pointed to the importance of (additional) supervision or a different form of supervision. In the end, the legislator did not opt for a committee comparable to the CTIVD. Arguments for this were the existing supervision by an examining magistrate and supervision by the Central Review Committee of the Public Prosecution Service. Instead, the Justice and Security Inspectorate has been chosen, which supervises cases that are and are not submitted to the court.

Based on our research, we do not take a position on this discussion. However, it is worth noting that if the role of oversight for hacking power is explored further, there are a number of countries that have surfaced from the study that may provide guidance.

Firstly, it is relevant in this context that Belgium and France have examining magistrates overseeing the execution of the hacking power. The Examining Magistrate granting authorisation for the deployment of the hacking power also supervises the execution thereof. If needed, the Examining Magistrate may decide to terminate the hacking operations. This oversight goes beyond the role of the Examining Magistrate in the Netherlands, who principally only oversees the hacking power prior to deployment. The working method in Belgium and France solves the problem that part of the cases are not presented to court. As a side note, it should be noted that the examining magistrates rely on the information provided. The question is thus whether this judicial

oversight actually results in a substantive review during deployment. It does however offer a perspective that deviates from the Dutch system in which the Examining Magistrate grants an authorisation prior to the deployment and thereafter generally no longer oversees the hacking operations.

Secondly, also relevant is the Swedish supervisor SIN. This supervisor specifically oversees the execution of the hacking power. It is therefore similar to the Committee modelled on the CTIVD as proposed by some authors. As yet, SIN's supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness and it oversees both the police activities as well as those of the Public Prosecution Service. As such, it distinguishes itself from the tasks of the Inspectorate in the Netherlands, which only oversees the police. SIN can furthermore issue public statements in individual cases upon request or on its own accord. Given that SIN focuses both on the legal and process-related aspects, this solves the issues raised earlier that not all cases are heard by a session judge and that the judge is not always sufficiently capable of properly assessing the evidence.

Scenario 3: Customised examination

As previously discussed, the examination in the Netherlands constitutes an important safeguard in the deployment of technical tools and the quality of the data collected by means of the tools. Practice shows that the examination and the use of technical tools do not always proceed as intended by law. Technical tools that are mainly used are tools that are not pre-approved and technical tools that cannot be approved due to their nature. Notably, the safeguards relating to technical tools and the data quality are less detailed by law abroad than in the Netherlands. In that respect, it is easier to deploy the hacking power abroad. Another striking aspect is that there is little or no case law available that challenges the use of the hacking power in these countries. This incidentally does not mean that the evidence provided by the hacking power will always be readily accepted. In many countries, the hacking power is relatively new and its use and any opinions thereof will continue to develop. Therefore, it cannot be ruled out that future rulings may still ensue that will impact the current legal framework in these countries. This does not detract from the interesting fact that several countries have chosen not to check data quality in a way that is done in the Netherlands. And that the working method in those countries has, as yet, not resulted in any fundamental discussions in the courts. It is for this reason that we have included a third scenario which takes a more tailor-made approach to the examination requirements, with attention to additional tactical and technical safeguards. This scenario explores a) the use of a risk analysis for the examination and b) the question to what extent additional tactical and technical measures are adequately safeguarded.

Scenario 3a: Risk analysis in the examination phase

Risk analyses form part of the decision to purchase and use technical tools in Germany. An SLB guideline addresses various themes that should be taken into consideration when it involves technical tools, such as the testing policy. A risk analysis identifies which objects pose a risk for these themes and what additional measures are needed. The different parties involved must conform to this. In the Netherlands, the performing party Digit indicates that the Dutch National Examination Service, as well as the underlying inspection protocol, does not take sufficient account of the fact that it could also operate on the basis of a risk analysis, namely in terms of the measures it takes when deploying a technical tool. It is particularly this risk

analysis that appears to have taken centre stage in Germany. Therefore, the working method in Germany could be further explored to see what lessons can be learned from it in terms of the Dutch situation.

Scenario 3b: Assurance of additional tactical safeguards in the Netherlands

As noted, the Netherlands currently mainly uses technical tools that, according to the Public Prosecutor, cannot be approved due to their nature. Tactical and technical measures are taken to safeguard the data quality in this situation. There are no indications at present that the use of commercial products will be terminated. The current Minister considers this to be a 'reality that we have to deal with', as evidenced by the committee debate on 7 July 2022. The use of risk analyses described in scenario 3a may serve as a guideline to take appropriate additional measures to ensure data quality. If the working method with commercial products remains the rule rather than the exception and the method will be continued by exactly the same token, it will also be important to review the role of the Public Prosecution Service with regard to the additional safeguards, tactical or otherwise. At present, the Public Prosecution Service is the only one checking these safeguards prior to a deployment. A tactical public prosecutor leading the criminal investigation is in principle ultimately responsible for the tactical safeguards. These are also reviewed by the Digit public prosecutor and the Central Assessment Committee of the Public Prosecution Service. Owing to the sole involvement of the Public Prosecution Service and no other independent bodies, it is useful to explore which other party can (additionally) verify the adequacy of these measures, especially when a case is not presented to court.

1 Introduction

1.1 Introduction

The Dutch Computer Crime Act III (CCIII) came into effect on 1 March 2019. Among other things, this Act introduces the power of the police to carry out hacking operations. The new Sections 126nba, 126uba, 126zpa in the Code of Criminal Procedure will allow specially authorised investigating officers to covertly and remotely intrude into computer systems under certain conditions and investigate them. A computer system is 'a device or group of interconnected or related devices, one or more of which automatically process computer data on the basis of a programme'.[1] Examples of computer systems include: smartphones, laptops and routers.[2] After having hacked a computer system, the police can carry out investigative actions such as the implementation of an order as referred to in Section 126l of the Code of Criminal Procedure (directly listening in on conversations) and Section 126m of the Code of Criminal Procedure (wiretapping) and recording data. The investigative actions can be carried out by means of a technical tool.[3] Within the meaning of the Decision on intruding into automated information systems (hereinafter: Decision), a technical tool is a 'software application that detects, registers and transports data, and with which investigative actions can be conducted in execution of an order'.[4] Somewhat briefly, this definition implies the following: a technical tool, which is mostly software, detects data, i.e. an e-mail on a suspect's phone, and forwards them to the police.

The Computer Crime Act III contains several other grounds which can be used as the basis for establishing rules regarding the implementation of authorised hacking under or pursuant to an Order in Council. Based on Section 126ee of the Code of Criminal Procedure, the Decision has formulated rules regarding the investigative actions being carried out with the use of a technical tool. These rules are designed to help ensure that the hacking power is not abused and that the authenticity and integrity of the data obtained can be assured.[5] The Decision contains rules formulated in respect of the expertise and authorisation of investigating officers, on the recording of data for the implementation of an order and in respect of the technical requirements that have been set for a technical tool and how it should be examined. Other rules have been formulated that pertain to the performance of investigative actions in computer systems and the provision of data obtained during the investigation.[6]

As stated, one of the themes in the Decision concerns the examination of technical tools.[7] The Decision stipulates that a technical tool must be examined before it can be used.[8] There are exceptions to this rule.[9,10] The explanatory notes to the Decision

1 Section 80e of the Dutch Criminal Code.
2 The term automated information system is a broad definition and may pertain to many different devices. A 'group of interconnected devices' is also considered to be an automated information system (Van Uden & Van den Eeden, 2022).
3 It is not 'strictly necessary' to make use of technical tools. Actions will sometimes be performed in an 'ad hoc and manual' way (Bulletin of Acts and Decrees 2018, 340, page 16).
4 Bulletin of Acts and Decrees 2018, 340, page 2.
5 Parliamentary Papers II 2015/16, 34 372, no. 3, page 54.
6 Bulletin of Acts and Decrees 2018, 340, page 13.
7 Chapter 3.1 discusses this in more detail.
8 Article 14 of the Decision on intruding into automated information systems (hacking).
9 Article 15(1) of the Decision on intruding into automated information systems (hacking).
10 Article 15(2) of the Decision on intruding into automated information systems (hacking).

demonstrate that, if the police intend to use a technical tool, this technical tool initially has to be examined and approved.[11] Following the approval, the technical tool is assigned a number that can then be used throughout the criminal investigation and for the criminal investigation file. Such a number obviates the need for the police to report any information about the composition and operation of the technical tool. This protects the interests of the investigation.[12] Since 2020, the Dutch National Examination Service, which forms part of the National Police's Specialist Operations Unit, takes care of the inspections.

The Inspectorate of Justice and Security oversees compliance with the manner in which the police execute the hacking power. In its first report in 2019, the Inspectorate of Justice and Security concluded that none of the six cases in which the police had been granted power to carry out hacking operations had deployed a pre-approved technical tool. Additionally, there was one case in which the technical tool had been submitted for examination afterwards. In the other cases, the technical tools have not been submitted for examination.[13] A Letter to Parliament of the then Minister of Justice and Security indicates that there are a number of reasons why examination does not take place, or only to a limited extent. One of the reasons was to relate to the limited experience in the development and procurement of technical tools. Also, the report of the Inspectorate of Justice and Security shows that it is more difficult to examine commercial tools as suppliers are not prepared to give (full) access to their tools.[14] In his response, the Minister also indicates that the decision not to have a technical tool examined should be the 'exception to the rule' and not be made 'lightly', as reliability, integrity and traceability of the data collected are 'crucial' principles.[15] In his Letter to Parliament, the Minister commits that there will be an additional study into the manner in which other countries with which the Netherlands closely cooperates have organised the use of technical tools. The results may serve as input for the broader evaluation of the Computer Crime Act III[16] and also supplement the previously published evaluation on police hacking in the Netherlands. This report is the result of the additional research committed by the Minister.

1.2 Objective and question

The study's objective is to gain international insight into the legal frameworks set in place in different countries for the deployment of authorised hacking and for the technical tools that are or could be applied for this. If countries do not have separate laws and regulations governing the use of technical tools, the aim is also to find out whether there are other safeguards that ensure the reliability, traceability and integrity of the data being collected by means of the hacking power.

11 Bulletin of Acts and Decrees 2018, 340.
12 Bulletin of Acts and Decrees 2018, 340, page 20.
13 Inspectorate of Justice and Security, 2020, pages 8-9. The two subsequent reports also show that the majority of technical tools are not submitted for testing. However, there has been a slight increase in the use of pre-approved technical tools and more technical tools have been submitted for testing (Inspectorate of Justice and Security, 2021, page 9; Inspectorate of Justice and Security, 2022, page 7).
14 *Parliamentary Papers II* 2019/20, 29 628, no. 970, pages 2-3. This is also evident from the evaluation of the Research and Documentation Centre (WODC) on the execution of authorised hacking in the Netherlands (Van Uden & Van den Eeden, 2022).
15 *Parliamentary Papers II* 2019/20, 29 628, no. 970, page 3.
16 *Parliamentary Papers II* 2019/20, 29 628, no. 970, page 4.

The central research question for this study is as follows:
What safeguards govern hacking powers abroad, more specifically the use of technical tools, and how does this compare with the Dutch situation?

The central research question is answered on the basis of the following subquestions:
1 What countries allow 'authorised hacking' and on the basis of which legal ground can foreign police services carry out hacking operations in their own country?
2 What statutory conditions apply in other countries for police services to deploy the hacking power?
3 To what extent do other countries examine technical tools and what has been laid down in legislation and regulations on this?
4 To what extent are there any other rules to ensure the reliability, traceability and integrity of data obtained with the use of technical tools?
5 How does the working method abroad compare with the Dutch working method regarding the approval of technical tools and any other safeguards to achieve data reliability, integrity and traceability?

1.3 Research methods

1.3.1 Wide-ranging inventory and selection of countries

This study was an international comparative study. For the benefit of the study, a wide-ranging inventory was drawn up to identify the countries that have set up a statutory power for the police to carry out hacking operations. In order for this to be a hacking power, we adopted the premise that the hacking power takes place covertly and remotely. In the context of the wide-ranging inventory, nearly all European countries plus the United States, Canada and Australia have been reviewed.[17] There were (outdated) overviews available in literature of countries having established a hacking power.[18] The wide-ranging inventory had to provide an up-to-date overview of the countries allowing authorised hacking and the manner in which those countries ensured data quality.

Five countries were selected for a more detailed study based on the wide-ranging inventory.[19] The following criteria played a role in the selection process: 1) the presence of a hacking power, 2) the presence of an examination procedure, 3) an authority performing an examination or test of technical tools and 4) any other measures set up to help ensure data quality.[20] Also, a pragmatic argument weighed in. It turned out to be complicated, time-consuming and at times impossible to sufficiently liaise with each country that fit the selection. This is why Spain, Denmark and the United Kingdom were left out of the selection. Table 1.1 shows which countries could be studied in more depth, including a motivation to select the country in question.

17 The United States, Canada and Australia are interesting as the Dutch police cooperate with these countries.
18 See inter alia: Eurojust (2016) and Gutheil, Liger, Heetman, Eager and Crawford. (2017).
19 The wide-ranging inventory and the in-depth analysis of the five countries partly took place in parallel, due to the time it took to conduct a full wide-ranging inventory.
20 In his Letter to Parliament, the Minister explicitly agreed to study the working method of those countries the Dutch police closely cooperates with (*Parliamentary Papers II 2019/20, 29 628, no. 970, page* 4). However, we have not relied solely on this criterion in selecting the countries. A possible risk of using only this selection criterion was that potentially interesting countries would be missed out, countries which, for example, have established an examination process or which use other measures to ensure the reliability, integrity and traceability of data.

Table 1.1 Motivation for the selection of countries

Country	Motivation
Belgium	Has a statutory hacking power.
	The law refers to 'appropriate means' in connection with the confidentiality and integrity of data.
Germany	Has a statutory hacking power.
	Presence of an organisation (ZITiS) engaged in the development and research of technical tools.
	Different safeguards in place with regard to the use of digital data.
France	Has a statutory hacking power.
	Presence of an organisation (STNCJ) which monitors the quality of the technical tools in use.
Sweden	Has a statutory hacking power.
	Presence of an organisation (SIN) which monitors the quality and deployment of the hacking power.
Switzerland	Has a statutory hacking power.
	The law imposes conditions on the technical tools to be used, such as logging and the disclosure of the source code.

1.3.2 Research methods

Different research methods have been used to answer the research questions: document studies (laws and regulations and relevant (grey) literature), written questionnaires and interviews. Appendix 1 lists the sources consulted for each country. The text below further explains the research methods.

Legislation, regulations and literature review
Current laws and regulations were studied for this research. In addition, we analysed literature discussing legislation and regulations. In doing so, we used both grey literature and scientific articles, found via Google (Scholar) and digital libraries that could be consulted via Rijksportaal (the government portal). News articles were sometimes also consulted, for example because it discussed technical tools which the police were to make use of in a particular country. Relevant documentation was found not only through search engines, but also via the people we interviewed (see below). We then used the snowball method to find and study supplementary literature (Boeije, 2008). We tried to consult as many English-language documents as possible. If this proved impossible, we made use of Google Translate, which translated the document in question into English. Only occasionally did we consult a native speaker who provided us with a translation. Apart from the literature and legislation and regulations, we also searched for available case law. The emphasis was on available case law that focused on the quality of the data obtained by means of hacking operations. Due to the large number of countries in this study, it was not possible to carry out a case law study for each individual country. Instead, we made use of the respondents in this study and asked them whether there was any relevant case law. Our inventory of relevant case law is thus not exhaustive.

Mailing experts
A short questionnaire was sent out via Eurojust (the *European Union Agency for Criminal Justice Cooperation*) for the purpose of the wide-ranging inventory. Eurojust brings together prosecutors and judges from across the EU and beyond, in an effort to effectively tackle all forms of serious cross-border crime (Eurojust, undated). Furthermore, Eurojust is a key partner of the European Judicial Cybercrime Network (ECJN), a network established to improve cooperation between judicial authorities on cybercrime, digitalised crime and digital investigation (Eurojust, undated). By courtesy of Eurojust, the European member states were presented with four questions on the following topics: the presence of a (statutory) hacking power, relevant legislation and regulations and literature, the presence of an examination process for technical tools and any other measures that need to be taken to ensure data quality. Fourteen out of 26 countries completed the questionnaire. The fact that the questionnaire was not part of a mandatory 'questionnaire' may explain why not all countries completed the questionnaire. In the case of a mandatory questionnaire, all countries forming part of Eurojust are obliged to respond.

Interviews
For the purpose of the wide-ranging inventory, exploratory interviews took place with scientists working on cyber-related themes and the deployment of (new) investigative powers. The interviews were held in the period between February 2022 and December 2022. In some cases, we approached the interviewees in response to an actual publication, at other times we learned about them through a general e-mail address of a faculty engaged in a field relevant to us. We also held a number of exploratory interviews with practitioners in the field of cyber-related cases such as public prosecutors, police officers or lawyers.[21] These interviews were usually initiated after these persons had been suggested to us by the scientists that we contacted or when we failed to receive a response via the short questionnaire sent out via Eurojust. We also occasionally had additional questions following the short Eurojust questionnaire. In the end, we conducted twenty exploratory interviews with twenty-two respondents. Most interviews related to one country. In a few cases, two or three countries were discussed in the interviews. Sometimes, it proved impractical to conduct an exploratory interview, for example due to busy schedules of those potentially to be interviewed or because they preferred to receive a questionnaire by e-mail. In those cases, we asked a number of questions relevant for the wide-ranging inventory per e-mail. We sent nine additional questionnaires per e-mail.

During the exploratory interviews and e-mail questionnaires, we, inter alia, asked questions about the presence of the hacking power, the use of technical tools, any measures in the context of the quality of the data collected or to be collected and possible court cases.

In addition to the exploratory interviews discussed above, we also conducted in-depth interviews with persons in the five countries that we had selected. The aim of these in-depth interviews was to obtain a more comprehensive overview of the manner in which the statutory hacking power was set up in that particular country. We contacted these persons via earlier contacts, i.e. by means of the snowball method. In principle, for each country, we spoke with a representative of the ministry responsible for legislation in the area of investigative powers, hacking more specifically, and with representatives of the Public Prosecution Service, the police and organisations involved

[21] Incidentally, the difference between scientist and practitioner was not always clear-cut. Occasionally, a person was both scientist and practitioner, for example a lawyer.

in the supervision of hacking operations/the use of technical tools.[22] For these interviews too, we sometimes limited ourselves to a questionnaire via e-mail, partly because the person or organisation concerned preferred this, due to the confidential nature of the subject matter. On rare occasions, one of these officials did not want to speak with us or answer any questions via e-mail. In total, we conducted fourteen in-depth interviews and sent out three in-depth questionnaires.

During the interviews, we addressed the topics that also featured during the exploratory interviews. We additionally included questions targeted towards the respondent's position. We also added questions on topics that had not become sufficiently clear based on previous interviews and the analysis of relevant documents.

Limitations
The selected research methods are subject to several limitations. First, our research focuses on the legally defined requirements. This subsequently meant that formal and informal policy rules, for example those applied by the police with regard to the processing of data obtained, were excluded from this study. Where available, we did include information about the policy rules, though in most cases, the policy rules, insofar as present, turned out to be confidential and not publicly available. This study is thus mainly a representation of the statutory provisions in the different countries. Second, we refer to available case law in this report. We did not conduct a full case law study, partly due to time constraints. Instead, we base ourselves on available literature and interviews. The inventory is therefore not exhaustive and this study provides an initial overview of case law that may or may not be present. Finally, this study focused on remotely and covertly hacking computer systems. The physical hacking operations of devices were thus beyond the scope of the present study.

1.4 Analysis

The moment a significant part of the data had been collected, we proceeded with the analysis. In the meantime, some preliminary analyses were also performed to ensure the right questions were asked during the in-depth interviews. A list of codes was prepared in Word for the principal analysis. These codes were based on the main elements resulting from the research questions. Examples of codes included the legal ground, investigative actions, examination or other measures needed to ensure data quality. The code list also included statutory conditions such as the types of criminal offences and the period within which the hacking power could be deployed. A code list was drawn up for all countries. This task was divided among the three researchers. This included the possibility of also adding codes if they proved relevant to the country in question. Given the volume of the information, we did not use an analysis programme such as Maxqda for example; instead the analysis took place manually.

Based on the code lists per country, we drew up a general overview of the different countries (Chapter 2) and five selected countries are described in more detail (Chapters 3 to 7).

[22] It was not always clear beforehand whether a person worked at the Public Prosecution Service or for the Ministry. In France, for example, it is customary for a person to work as a public prosecutor for a number of years, followed by a number of years working for at the ministry. This is the reason why we spoke with two persons of the ministry in France and not with a representative of the Public Prosecution Service.

1.5 Structure of the report

This report is structured as follows. Chapter 2 has a country overview. First, the Chapter uses a country map to identify which countries have established a power of the police to carry out hacking operations. It also outlines the statutory conditions present. The second part of Chapter 2 contains a number of summary tables with safeguards set in place in the different countries with regard to enhancing the quality of the data collected. Chapters 3 to 7 inclusive contain detailed descriptions of the countries selected by us. These descriptions feature Belgium, Germany, France, Sweden and Switzerland, respectively. Chapter 8 focuses on the conclusion. The conclusion compares the countries selected by us. Where possible, comparisons are made with the situation in the Netherlands. This chapter ends with a number of scenarios.

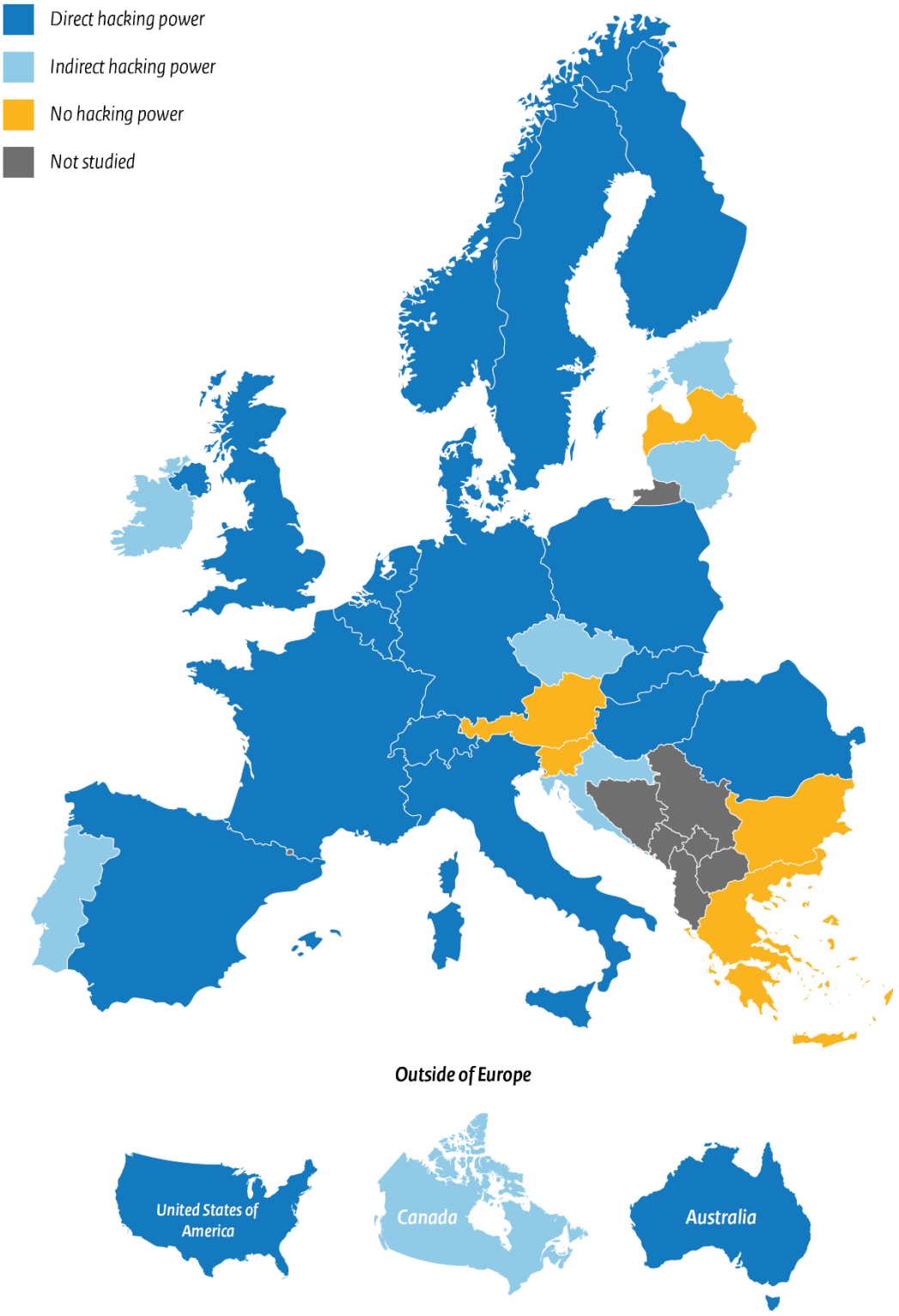
2 Country overview

This Chapter provides an overview of the presence of hacking powers with respect to a large number of European countries, Australia, Canada and the United States. Section 2.1 focuses on the question as to whether a country has introduced hacking powers, including the conditions applicable to deploy such powers, as well as the investigative actions that may be undertaken. This section starts with a figure illustrating which countries allow authorised hacking. This is followed by an overview of a number of conditions. Section 2.2 then explains the safeguards put in place in different countries to ensure the quality of the data collected. While this chapter does not yet draw a comparison with the Netherlands, the Netherlands is included in the various tables, for information purposes.

2.1 Presence of hacking powers and conditions

Figure 2.1 features a map of all the countries included in this study. The figure indicates whether a country has set up a statutory power of the police to carry out hacking operations, and if so, whether this is a direct or indirect power. A direct power applies if the law explicitly refers to the possibility of covertly and remotely intruding into a computer system and undertaking one or more investigative actions within that system. An indirect power applies if the hacking power forms part of a general provision. Consider, for example, the power to intercept telecommunications, whereby the law text does not specifically mention the hacking power, though the power could be used for that purpose.

Figure 2.1 Country overview - hacking power



The maps are adaptations of works by Maix (Europe; CC BY-SA 3.0), Theshibboleth/Lokal_Profil (VS; CC BY-SA 2.5), Paul Robinson/Lokal_Profil (Canada; public domain) and Rycherr (Australia; CC BY-SA 4.0 and previous versions).

By deploying the hacking power, the police in these different countries are allowed to carry out various investigative actions. Appendix 2 further specifies these actions for each of the different countries. The table below presents the three most common investigative actions. These are 1) the search and storage of data on computer systems, 2) the interception of telecommunications, such as audio, footage, internet traffic, and 3) surveillance activities such as activating the microphone, camera or GPS on the computer systems. The table also indicates if the law does not specify what actions may or may not be carried out when deploying the hacking power.

Table 2.1 Investigative actions hacking power

Country	Search	Interception	Surveillance	No requirements
Australia	X			
Belgium				X
*Bulgaria**				
Canada				X
Denmark				X
Germany	X	X		
Estonia				X
Finland	X	X		
France	X	X		
*Greece**				
Hungary	X	X	X	
Ireland	X		X	
Italy		X	X	
Croatia	X	X	X	
*Latvia**				
Lithuania				X
Luxembourg		X		
The Netherlands	X	X	X	
Norway	X	X	X	
*Austria**				
Poland	X	X	X	
Portugal	X	X	X	
Romania	X	X	X	
*Slovenia**				
Slovakia	X	X	X	
Spain				X
Czech Republic				X
United Kingdom	X	X	X	
United States	X			
Sweden	X	X	X	
Switzerland		X		

* No hacking power.

Half of these countries have established all three investigative actions. Seven countries have not incorporated any prerequisites in terms of the investigative actions. In principle, that means that any action may be included in the order and that it is up to the court to decide whether it can issue an authorisation for this or not. Lastly, the country overview considered whether there is any case law available (not based on a full case law analysis) that raises the issue of the quality of the data obtained by means of hacking operations. Interestingly, as far as we know, only two countries, i.e. France and Sweden, have case law in which data quality has been disputed. It may be concluded that data quality is not called into question. However, it cannot be ruled out that these discussions do take place but are not reflected in court decisions, making them more difficult to find. Based on their own experience, interviewees said they knew of very few cases where data quality was called into question. According to them, this could be partly due to a lack of technical knowledge on the part of the defence and/or the additional (conclusive) evidence presented. Perhaps future case law will lead to legislative adjustments, such as the tightening of safeguards regarding the quality of the data collected. Such a situation took place in France where a certificate of authenticity may have to be issued as an additional safeguard by the service exercising the power and securing the data. For a more detailed discussion, see Section 5.9.[23]

2.2 Safeguards with regard to the data collected

This section discusses the statutory safeguards applicable to data being collected by means of a hacking power. These are essentially safeguards specifically mentioned in the legal provision laying down the hacking power or mentioned in other legal provisions associated with the legal provision on the basis of which the police may carry out hacking operations. Where possible, informal safeguards are addressed, for example from internal policy rules or best practices applied by the police. As these safeguards are informal in nature and by no means always laid down formally and/or because we were unable to get a clear overview of them during our research, this study focusses on those safeguards which are regulated by law.

The inventory identified the following categories of safeguards:

- Presence of an examination of technical tools by an independent authority.
- Presence of an independent authority specifically concerned with monitoring the deployment of the hacking power. General inspectors, who focus on the police task as a whole, for example, are excluded from this inventory.
- Rules regarding the documentation and logging of investigative actions carried out to ensure that those actions carried out are transparent and traceable.
- The presence of judicial supervision. At issue is not whether deployment requires a magistrate's prior authorisation, but whether there is a court judge or otherwise supervising the execution of the hacking power during the period of the deployment.
- Rules regarding the storage of data collected by means of hacking operations.
- Conditions that apply if a case is taken to court and the manner in which the suspect's right to inspection is formulated.

The text below focuses on the main findings that emerged from the inventory. The next summary tables only include those countries that have actually established a hacking power. Appendix 3 has a more extensive table with an overview of the

[23] Court of Cassation, criminal division, 11 October 2022, appeal no. 21-85.148.

safeguards applied by the different countries regarding the data collected with the use of hacking operations.[24]

2.2.1 *Examining the technical tools and supervisory body*

Table 2.2 Presence of examination and supervisory body

Country	Examination	Supervisory body
Australia	No	Ombudsman
Belgium	No	No
Canada	No	No
Denmark	No	The Danish Independent Evidence Supervisory Board
Germany	No	The Central Office for Information Technology in the Security Sector (ZITiS)
Estonia	No	No
Finland	No	No
France	No	Service technique national de captation judiciaire (STNCJ)
Hungary	No	No
Ireland	No	No
Italy	No	No
Croatia	No	No
Lithuania	No	No
Luxembourg	No	No
The Netherlands	Yes	Dutch National Examination Service
Norway	No	Controlling committee coercive measures
Poland	No	No
Portugal	No	No
Romania	No	No
Slovakia	No	No
Spain	No	No
Czech Republic	No	No
United Kingdom	No	Investigatory Powers Commissioner's Office (IPCO) & Investigatory Powers Tribunal
United States	No	No
Sweden	No	Commission on Security and Integrity Protection (SIN)

[24] Appendix 1 provides an overview of the different sources that have been consulted for the information in the overview.

Country	Examination	Supervisory body
Switzerland	No	No

None of the countries has established an examination by an independent examination body in charge of examining the technical tools before they are deployed based on a comprehensive examination protocol. Some countries do have a testing procedure, however, these procedures are not performed by an independent examination body. Furthermore, for those other countries that do have an examination or testing procedure, it is unknown what the procedure consists of. Germany constitutes an exception in this regard. Even in that country, it is not entirely clear what the testing entails, but it is clear that it is based on an SLB guideline specifically designed for it. See Section 4.8.

In other countries, the supervision of hacking operations by an independent body is limited, thereby not including the trial court. Australia, Denmark, Norway, the UK and Sweden have independent bodies performing some level of supervision of the execution of the hacking power. Owing to its technical expertise, Germany has an authority that advises on the deployment and development of technical tools. France has a specific authority responsible for the design, supervision and implementation of technical tools used for hacking operations. The authorities in Sweden, Germany and France will be discussed in more detail in the coming chapters.

Table 2.3 Safeguards for documentation, storage and judicial supervision

Country	Safeguards for the documentation of actions	Judicial supervision during deployment	Safeguards for the storage of data
Australia	Yes	No	Yes
Belgium	Yes	Yes	Yes
Canada	Yes	No	No
Denmark	Unknown	No	No
Germany	Yes	No	Yes
Estonia	Yes	No	No
Finland	Unknown	No	Yes
France	Yes	Yes	Yes
Hungary	Yes	No	Yes
Ireland	Unknown	No	No
Italy	Yes	No	Yes
Croatia	Yes	Yes	Yes
Lithuania	Yes	No	No
Luxembourg	Yes	No	Yes
The Netherlands	Yes	No	Yes
Norway	Yes	No	Yes
Poland	Yes	No	Yes

Country	Safeguards for the documentation of actions	Judicial supervision during deployment	Safeguards for the storage of data
Portugal	Yes	Yes	Yes
Romania	Yes	No	Yes
Slovakia	Yes	No	Yes
Spain	Yes	Yes	Yes
Czech Republic	Yes	No	Yes
United Kingdom	Yes	No	Yes
United States	Yes	No	Yes
Sweden	Unknown	No	No
Switzerland	Yes	No	Yes

Almost all countries require some sort of documentation with regard to documenting and logging operative actions. As a minimum, they require an official report documenting all actions. Some countries take it a step further and require the logging of all actions. During our research, it remained unclear to what extent five countries have requirements to document and register operative actions. There is judicial supervision in Belgium, France, Croatia, Portugal and Spain *during* the deployment of the hacking power. This means the police must provide interim updates on progress to the judge who issued the order. In some cases, the judge may withdraw the authorisation for the hacking operations based on those status updates. As far as we know, there is no interim judicial review in the remaining countries.

Twenty countries have included safeguards in their laws regarding the storage of data collected with the use of hacking powers. These safeguards include the sealed storage of data or the storage of data in a secure environment. In the case of the remaining countries, nothing is included in the law or it has not become clear to us whether countries have set formal or informal safeguards.

2.2.2 *Trial and right to inspection*

Table 2.4 The notification obligation and right to inspection

Country	The notification obligation	Right to inspection
Australia	No	No
Belgium	Yes	Yes
Canada	Yes	Yes
Denmark	Yes	Yes
Germany	Yes	No
Estonia	Yes	Yes
Finland	No	No
France	No, only at the start of the court case	Yes
Hungary	No	No

Country	The notification obligation	Right to inspection
Ireland	No, unless made compulsory by the court	No
Italy	No	Yes
Croatia	Yes	Yes
Lithuania	Yes, unless it harms the interest of the investigation	Yes
Luxembourg	No, only at the start of the court case	Yes
The Netherlands	Yes	Yes
Norway	Yes, unless a state secret is involved	Ja
Poland	No	No
Portugal	Yes	No, only if public
Romania	No	Yes
Slovakia	No	Yes
Spain	No	Yes
Czech Republic	Yes	Yes
United Kingdom	No	No
United States	No	No
Sweden	Yes, unless it harms the interest of the investigation	Yes
Switzerland	Yes	Yes

Thirteen countries have included a notification obligation in the law. This means that those persons whose computer system was hacked must be informed within a predefined term that this hacking power had been deployed. In half of these countries, notification can be deferred or sometimes even omitted if the interests of the investigation may be compromised. In nearly all countries, the suspect will be notified if the case is brought before the court. Seventeen countries have explicitly included the right to inspect obtained data in legislation. In many cases, the defence may receive a copy of the data obtained. Among the remaining countries, our inventory did not show whether this hacking power is covered by a specific legal provision regarding the right to inspection.

Introduction to the country chapters

The coming chapters contain a description of our selected countries. Successively we discuss Belgium, Germany, France, Sweden and Switzerland.[25] For each country, we provide a description of how hacking powers are regulated. We largely follow the classification of Corstens and colleagues (2018). That means we discuss the following topics for each country: an description of how the hacking power is defined, the competent authorities and the corresponding process. We also focus on the persons and computer systems against whom/which the power may be used. It then focuses on the type of crimes (the cases), the time of authorisation and the formalities. We then pay attention to the technical tools that may be used and the safeguards that apply, especially with regard to the quality of the data collected. We always conclude with available case law and a brief concluding comment.

In order to compare the countries just mentioned and the Netherlands, the introduction first describes the Dutch situation. This involves a very brief description of the legal framework. In addition, the various safeguards in place in the Netherlands to ensure the quality of the data collected are discussed. The implementation process is also considered. The latter is important for a meaningful comparison between the Netherlands and other countries (see chapter 8). A detailed description of the Dutch situation can be found in in a previously published WODC-report (Van Uden & Van den Eeden, 2022) and in Annex 4 of this report. The information described in this chapter is based on findings on the previously published WODC-report (Van Uden & Van den Eeden, 2022).

Statutory regulation in the Netherlands

The Computer Crime Act III (Wet computercriminaliteit III – hereinafter: the CC Act III) came into force on 1 March 2019. The new investigative power allows a special law enforcement team 'to access computer systems remotely by stealth, under certain conditions, that are used by suspects, with a view to certain investigative objectives in the area of the investigation of serious criminal offences'. After accessing a computer system (such as a mobile phone or a server) the police may carry out a number of investigative activities which are mentioned in Section 126nba (1) CCP.

Both technical and tactical actors are involved with the power and its implementation, the former represented by Digit (Digital Intrusion Team). Digit itself consists of two components: Digit (Police) and Digit (Public Prosecution Service). Implementation of the hacking power is in the hands of Digit (Police), part of the Central Unit of the Dutch national police. Digit police is managed and led by Digit Public Prosecution Service, which is part of the National Public Prosecutors' Office of the Public Prosecution Service. Any intervention with the hacking power by Digit takes place within an ongoing criminal investigation, which is carried out by a tactical police team (such as a team of the district criminal investigation team or the National High Tech Crime Unit) under the authority of the Public Prosecutor handling the case. This Public Prosecutor bears ultimate responsibility for the criminal investigation in which Digit

[25] See chapter 1 for an explanation of the selected countries.

carries out an intervention, and he/she is accountable to the court when the case is heard by a judge in a trial court.

In order to conduct investigatory actions, technical tools may be used. In principle, law enforcement must make use of a technical tool that has been examined and approved in advance by the Examination Service. In the Netherlands there are detailed regulations about regarding measures to ensure the quality of the data collected. A significant part of this is contained in the Decision.[26] Measures mainly concern the period prior to deployment, but safeguards can also be distinguished with regard to the period during and after a deployment of the hacking power.

Prior to deployment

In terms of the period prior to deployment, the Decision contains a variety of rules that a technical tool must satisfy. There are also rules for the technical infrastructure[27] used by the police to store the data. The Examination Service monitors – in principle prior to deployment – whether a technical tool meets all the requirements. When this is the case, a technical tool is approved for use. In such cases, a technical tool can be used by the law enforcement agency without providing any explanations about its operation. The Examination Service does not inspect the technical infrastructure used to store the data.

The requirements in the Decision create the existence of a legal framework in the Netherlands that provides precise details about how the quality of the data collected should be guaranteed. Practical experience, however, has proved that implementation is difficult to realise in practice. There are two reasons for this. First, it has scarcely been feasible in practice to develop in-house technical tools – and have them approved in advance – due to the considerable time and cost involved in developing a fully approved tool. From the Digit Police's point of view, the rules and requirements formulated are difficult to execute because they are not found to be well suited to the technical tools developed by the law enforcement agency. Digit Police also believe that not all the rules are necessary. If policy makers took risk analysis and evidential value as the starting points of their reasoning, it would not be necessary for a technical tool to meet all the examination requirements. But that is the legal necessity at the present time.

Second, Digit police have made use of a commercial product in the majority of their actions. Such a product is purchased by the police from an external supplier. This product is not subject to examination and approval, because the public prosecutor has decided that the very nature of this tool stands in the way of examination and approval, a decision that fits within the parameters of the legal framework. Based on the current Decision and the examination requirements as formulated, it will also never be possible to approve this kind of technical tool. That means that for a commercial product, too, it has not proved feasible to deploy a technical tool with prior approval. In order to, as yet, safeguard the quality of the data, the investigators engage additional tactical safeguards in practice. These are intended to allow verification of the data that has been obtained using the technical tool. The current

[26] Decision on intruding into automated information systems (hacking), 2018.
[27] Technical infrastructure refers to a 'technical provision of a technical team intended for recording data pursuant to execution of an order' (Decision on intruding into automated information systems (hacking), 2018, p. 2).

Decision does not take into account that such measures can be and are adopted in practice.

It is not yet clear at the present time how a judge hearing the case would rule on police actions performed with an unapproved technical tool. As far as we know, deployment of authorised intrusion has not yet been substantively addressed or raised for discussion at a court session. However some cases in which an attempt was made to use the hacking power or in which the hacking power was used have now been dealt in court (see for example Berndsen, 2022).[28]

During and after deployment

The Decision also foresees in a number of safeguards that must be in place during deployment of an authorisation. Not just anyone can be granted authorisation. This applies for example to persons who are permitted to perform investigatory actions with a technical tool, but also to persons who have access to the data collected. Another safeguard is logging. The purpose of logging is to determine precisely what actions were performed and whether any problems arose during implementation of the authorised intrusion order. After deployment of an authorised intrusion action, official police reports are added to the file, and the persons against whom the authorisation was deployed must be informed. A person does not have to be informed separately if the official police reports in the relevant file reveal that authorised intrusion was deployed. Finally, the Inspectorate's oversight forms a third safeguard. The Inspectorate takes into account a great many other rules in the Decision, and to what extent they have been complied with. Each year the Inspectorate publishes an Annual Report (public domain). The Annual Reports published thus far show that the police have not yet met all the requirements that have been laid down by or pursuant to the Decision.[29]

[28] Parkins-Ozephius et al (2022, p. 8-9) note that for technical devices covered by the 'old' Decision on technical tools criminal procedure, there are already several rulings. These rulings indicate that for the purposes of evidence, the lack testing is irrelevant. The future will have to show whether those rulings will be applied by analogy.

[29] The WODC report on the practice of implementing authorised hacking in the Netherlands (Van Uden & Van den Eeden, 2022) delves into the question of why the police do not always meet all the requirements. Further consideration of this issue lies outside the scope of this report.

3 Belgium[30]

Special thanks to Jan Kerkhofs (Public Prosecution Service, Belgium) for critical reading of this chapter for factual inaccuracies.

3.1 Statutory basis

On 25 December 2016, the Belgian parliament passed a law (sometimes referred to as the 'Cyber Christmas Law')[31] containing various amendments to both the Code of Criminal Procedure (CCP /*Wetboek van Strafvordering*) and the Penal Code (PC / *Strafwetboek*). One of the aims of this Law was to improve the existing special investigative powers. Two of the amendments allow hacking by the police, namely the extension of intrusive surveillance operations (an amendment to Articles 46*quinquies* and 89*ter* CCP) and the merger of covert searches in an information system,[32] referred to below as a computer system, with the interception of telecommunications (Article 90*ter* CCP) (Kerkhofs & Van Linthout, 2019, pp. 38-39), referred to below as data interception.[33] Because both powers (can) be applied from a distance (personal communication, June 9, 2023; June 14, 2023), they are discussed in more detail in this chapter. Since 2019, Belgium has also has an 'updated' Article 88*ter*. On the basis of this article, an investigating judge (*onderzoeksrechter*) can direct that a search in an information system instituted pursuant to Article 39*bis* CCP be extended to an information system or part of an information system that is located at a place other than that at which the search is being carried out. For this purpose, the security of the computer system can be breached, since Article 88*ter* CCP must, according to Kerkhofs and Van Linthout (2019, p. 372), be read together with paragraph 5 of Article 39*bis* CCP. As Article 88*ter* CCP 'should be viewed in the context of non-covert internet investigations (Kerkhofs & Van Linthout, 2019, p. 394), this article of the Law is not discussed in more detail in this chapter.

3.1.1 Intrusive surveillance operations

On the basis of Article 46*quinquies*, paragraph 1 CCP, police services agencies are entitled, after obtaining authorisation from an investigating judge, to enter a private place and open closed objects found there, either without the knowledge of the owner or entitled party or without their consent. For this purpose, a private place is deemed to mean a place other than a dwelling, an appurtenance to a dwelling within the meaning of Articles 479, 480 and 481 PC and premises used for professional purposes or the home of an attorney or a physician as referred to in Article 56*bis* CCP. Article 89*ter* CCP is an addition to this, as is apparent from the first paragraph of that article. This article enables police services agencies to enter a private place other than that referred to in article 46*quinquies* CCP. It also provides that, after authorisation has been obtained from an investigating judge, a computer system can be accessed and searched, either without the knowledge of the owner or entitled party or without their

30 For this chapter, we have made grateful use of the book by Kerkhofs and Van Linthout (2019).
31 Part of this Law was annulled by the Constitutional Court (*Grondwettelijk Hof*). This was why remedial legislation was passed in May 2019 (Royer & Yperman, 2020, p. 23).
32 As is apparent from the preparatory documents of the Computer Crime Law (*Wet informaticacriminaliteit*), information systems are deemed to be 'all systems for the storage, processing or transmission of data' (Royer & Yperman, 2020, p. 25).
33 See Annexe X, which includes a reference to the Belgian Code of Criminal Procedure.

consent (Article 89*ter* CCP). In principle, only an investigating judge can issue a warrant for intrusive surveillance in an information system. There is one exception to this provision, which is apparent from reading three provisions in conjunction with one another, namely Article 89*ter*, which refers to Article 46*quinquies*, paragraph 6 CCP, which in turn refers to Article 46*quinquies*, paragraph 3 CCP. A public prosecutor can order intrusive surveillance in a computer system, provided that this is not located in a dwelling and that it is not necessary to enter a dwelling for this purpose. In addition, the aim of a surveillance operation of this kind should be the installation of a technical device for observation purposes, for example the installation of a keylogger on a computer (personal communication, 24 March 2023).

An intrusive surveillance operation may be carried out only: 1) 'to ascertain the possible presence of items which are the object, means of committing or product of the offence or the pecuniary gains or replacement gains of the offence'; 2) 'to collect proof of the presence of such items (a specific copy of certain data)'; 3) 'to place or remove a technical device in the context of surveillance'; and 4) 'to replace objects that have been removed' (Yperman et al., 2019, p. 397). The legislature has not specified how entry can be gained to premises in the case of intrusive surveillance operations (for example, by the use of lock picks) (Kerkhofs & Van Linthout, 2019, p. 432).

It is apparent from Article 46*quinquies*, paragraph 2 (1) and (2) CCP that intrusive surveillance operations may be mounted in order to carry out a search 'in both the real world and the virtual world'. Objects may not be seized during such an operation (Kerkhofs & Van Linthout, 2019, p. 428). However, the operation may involve looking around to see whether certain evidence exists and taking 'a few samples'. Copying specific data would be permissible, but not copying a complete hard disk drive (Kerkhofs & Van Linthout, 2019, pp. 428-429). In the context of the non-digital world, this means that where an operation reveals the presence of, say, several kilos of cocaine, a small sample may be taken to prove their presence.

3.1.2 Data interception

The second statutory provision under which the police may carry out hacking operations is Article 90*ter* CCP. Under the first paragraph of this article, the investigating judge may authorise, 'for a covert purpose, the use of technical devices to intercept, view, search and record communications or data in an information system or part thereof that are not accessible to the public or to extend the search in an information system or part thereof.' This is referred to below as data interception. To make data interception possible, the investigating judge is authorised, under Article 90*ter*, paragraph 1, CCP, to issue a warrant to enter a dwelling or private place or gain access to a computer system. Every security device of the computer system in question may then be temporarily disabled, whether or not using technical devices, false signals, lock picks or false capacities. Finally, technical devices may be installed in the systems concerned in order to decipher and decrypt data stored, processed or transmitted by the systems. An example would be 'leaving behind snooping software or a remote access tool (RAT)[34] (Kerkhofs & Van Linthout, 2019, p. 462).

Although both powers (intrusive surveillance and data interception) enable the police to conduct hacking operations, Kerkhofs and Van Linthout wonder whether the power to carry out intrusive surveillance (Article 89*ter* CCP) will be used in practice. The

[34] A remote access tool (RAT) enables a person to penetrate and take control of a computer remotely.

activities that are possible in intrusive surveillance operations (looking around and taking samples) are much less far-reaching than in the case of data interception. However, requests to exercise each of these powers must be substantiated in the same (detailed) manner (Kerkhofs & Van Linthout, 2019, p. 431). In addition, a full preliminary judicial investigation must be instituted in the case of both these powers (personal communication, 24 March 2023). This raises the question of why the investigating judge would not immediately proceed to authorise the use of data interception (Kerkhofs & Van Linthout, 2019, p. 431).

3.2 Competent authorities

Both intrusive surveillance and data interception require the authorisation of an investigating judge, who 'communicates this to the public prosecutor'.[35,36] Unlike the situation in the Netherlands, there are two types of preliminary investigation in Belgium: criminal investigations (*opsporingsonderzoek*) and preliminary judicial investigations (*gerechtelijk vooronderzoek*). Criminal investigations are led by a public prosecutor *(procureur des Konings, Pdk*) The public prosecutor heads a district of the Public Prosecution Service (*Openbaar Ministerie*). A preliminary judicial investigation is conducted by an investigating judge (Traest, 2018, p. 25; p. 29). An important difference between the two types of investigation is that in a criminal investigation, 'save for certain statutory exceptions, the investigative acts may not involve the use of any coercive measure or the violation of individual rights and freedoms.'[37] By contrast, that is possible in the case of a preliminary judicial investigation. It should be noted, however, that in cases where a person is caught in the act of committing an offence or where the investigating judge issues a 'mini-instruction' for the performance of an investigative act (*mini-instructie*),[38] coercive measures may be applied in a criminal investigation (Traest, 2018, p. 25; p. 29). The Belgian Code of Criminal Procedure does not contain a comprehensive list of the powers assigned to the public prosecutor and to the investigating judge. Generally, however, there is no uncertainty about which of them exercises any particular power since there are two types of preliminary investigation and the power to carry out a number of investigative acts is explicitly assigned to the investigating judge (Traest, 2018, p. 25; p. 29).nThe Chamber of Indictment (*Kamer van inbeschuldigingstelling*) monitors, among other things, the manner in which the preliminary judicial investigation is carried out (*Ministère Public, no date*). As regards the actual exercise of the power, intrusive surveillance operations are currently the preserve of the National Technical and Support Unit of the Special Units Service (DSU-NTSU) of the federal police (Kerkhofs & Van Linthout, 2019, p. 432).
Data interception is carried out, in principle, by judicial police officers. They can arrange to be assisted by other staff of the judicial police and, subject to conditions set

35 Article 90*quater,* paragraph 1 CCP; article 89*ter* CCP.
36 There is one exception to this. Public prosecutors themselves may issue an authorisation to break into an automated work in order to install (and also repair and remove) a technical device with a view to carrying out observation as referred to in Article 47*sexies*, paragraph 1 (3) (Kerkhofs, & Van Linthout, 2019, p. 430).
37 Article 28*bis*, paragraph 3 CCP.
38 This instrument of a 'mini-instruction' for an investigative act (Article 28*septies* CCP) blurs the distinction between criminal investigations and preliminary judicial investigations. Nor is there any longer a link between the preliminary judicial investigation and the use of coercion. The instrument of 'mini-instruction' enables the Public Prosecution Service to request an investigating judge to give instructions for the performance of an investigative act that comes within his/her remit. A number of far-reaching acts are excluded from such instructions, namely the issuing of arrest warrants, search warrants and data interception warrants (Article 90*ter* CCP), the hearing of anonymous witnesses (Article 86*bis* CCP), observation of dwellings involving the use of technical devices (Article 56*bis*, paragraph 2 CCP) and intrusive surveillance operations (Article 89*ter* CCP) (Traest, 2018, pp. 32-33).

by the Crown, by administrative and logistics staff of the integrated police force.[39] This support was deemed necessary because the work involved in carrying out the investigative activities was considered at the time (then still mainly telephone taps) to be too labour-intensive for the implementing police services alone (Kerkhofs & Van Linthout, 2019, p. 478). However, some of the investigative activities cannot be left to the administrative and logistics support staff.[40] This applies to the analysis of the collected data. There is one exception to this, namely if they have a particular expertise. Nor may this group of staff be involved in selecting the parts of the communications considered important for the investigation, as referred to in Article 90*sexies*, paragraph 1 (2) CCP.[41] The police officers must record the names of those who assist them. A list is drawn up separately for each case file in accordance with rules determined by the Crown, after submission to a committee responsible for protecting privacy. Their names are not included in the file if they are merely following an order, as referred to in Article 90*ter*, paragraph 1 CCP.[42] The Royal Decree of 17 October 2018, published on 19 November 2018, lists conditions to be fulfilled by administrative and logistics support staff.[43,44]

3.3 Against whom?

Intrusive surveillance in a computer system can take place only in private settings where it is suspected, on the basis of precise information, that items may be found as referred to in Article 46*quinquies*, paragraph 2 (1) CCP (i.e. items related to an offence). Intrusive surveillance can also take place if it is thought that evidence can be collected or that private settings are being used by persons suspected of an offence (Kerkhofs & Van Linthout, 2019, p. 431).

As regards data interception, Article 90*ter*, paragraph 1 CCP provides that it must be clear whose computer system is to be investigated. That means that the following aspects can be considered: the identity of the suspect, the means of communication or computer system used by the suspect, the places where the suspect is regularly to be found and the persons with whom the suspect is in contact. On the basis of a judgment of the Court of Cassation (*Hof van Cassatie*), it is sufficient if one of these aspects is mentioned. For example, this means that, unlike the situation in the Netherlands (Van Uden & Van den Eeden, 2022, p. 37), where an authorisation is granted for person X not all telephones possibly used by X need be mentioned (Kerkhofs & Van Linthout, 2019, p. 452). If it becomes apparent during an investigation that its scope must be extended to another related computer system pursuant to Article 90*ter* CCP and that this should be done covertly, a fresh data interception warrant must be issued. If the computer system is located in a different

39 Article 90*quater*, paragraph 3 CCP.
40 These staff are generally referred to by their French name Ca-Log (Kerkhofs & Van Linthout, 2019, pp. 478-479). Ca-Log employees fulfill a civilian function and perform administrative, support or technical functions (Jobpol.be, n.d.).
41 This concerns: 'the duplication or reproduction of the parts of the recorded communications or data considered by the designated judicial police officers to be important to the investigation, and any translation thereof.'
42 Article 90*quater*, paragraph 3 CCP.
43 Royal Decree, 17 October 2018, Article 1.
44 Two conditions are specified. First, the staff concerned must have been designated by the chief of police (in the case of the local police) or by the director-general of the judicial police or his or her representative (in the case of the federal police). Second, the staff must have completed an internal training course for 'the use of technical devices for covertly intercepting, taking note of, searching and recording communications or data not accessible to the public or for extending such a search to an information system or part thereof.' The course must include 'aspects of data protection' (Royal Decree, 17 October 2018, Article 1).

country, the procedure specified in Article 88*ter*, paragraph 4 CCP must be followed (personal communication, 24 March 2023).

Article 90*octies*, paragraph 1 CCP provides that data interception can relate to 'premises used for professional purposes, the place of residence, means of communication or information systems of an attorney or physician' only if this recipient of confidential information is himself suspected of having committed or participated in an offence as referred to in Article 90*ter* CCP. Data interception can also be used 'if precise facts give rise to a suspicion that third parties suspected of having committed offences as referred to in Article 90*ter* make use of the premises, place of residence, means of communication or information systems of the attorney or physician concerned.' Some further conditions applicable to the interception of data in the possession of recipients of confidential information are set out in Article 90*octies*, paragraphs 2 and 3 CCP.

3.4 Cases

Intrusive surveillance in a computer system is possible if there are serious grounds for believing that an offence as referred to in Article 90*ter*, paragraphs 2-4 CCP has been committed. Such an operation can also be mounted if offences are being or might be committed in the context of a criminal organisation, as referred to in Article 324*bis* of the Penal Code (Kerkhofs & Van Linthout, 2019, p. 431).[45] This power may be exercised only if 'the truth cannot be established by some other means'.[46]
Data interception on the basis of Article 90*ter* CCP is possible for the offences listed in paragraphs 2-4 of that article. Paragraph 2 lists various offences (45 subparagraphs, each listing one or more offences). Examples are an attack on or conspiracy against the King, serious violations of humanitarian law, offences which violate constitutionally guaranteed rights and threats of an attack. Paragraph 3 deals with attempts to commit an offence, as listed in paragraph 2. Paragraph 4 contains an addition in respect of 'a band of criminals formed for the purpose of committing an attack on persons or property as referred to in paragraph 2 or committing the offence referred to in Article 467, paragraph 1.' This mainly concerns burglary committed by 'breaking and entering and the use of lock picks' (Kerkhofs & Van Linthout, 2019, p. 449).

3.5 Term of authorisation

An intrusive surveillance operation is intended as a one-off act (a 'one-time hit'). If it proves necessary to access a computer system for a second time, a fresh authorisation is needed (personal communication, 24 March 2023). A data interception authorisation is issued for a term not exceeding one month. This term starts on the day of the authorisation for the exercise of the power.[47] The starting date can be deferred for a maximum of two months until the moment when the power is first actually exercised. In this way, the time required to access a computer system, such as a telephone, is not counted towards the period during which the power may be exercised. This may be necessary as it may not always be (technically) possible to access a computer system (Kerkhofs & Van Linthout, 2019, p. 464). The term during which the power may be exercised may be extended for a maximum of one month at a time, subject to a

[45] Article 46*quinquies*, paragraph 1 CCP.
[46] Article 46*quinquies*, paragraph 1 CCP.
[47] Article 90*quater*, paragraph 1 (4) CCP.

maximum of six months in total. This maximum term of six months may be extended for a further maximum of two months if the exercise of the power has started later due to technical preparations.[48]

The authorisation should specify the 'precise circumstances which justify extension of the measure.' After the six-month period, the investigating judge may issue a fresh authorisation. That is possible if there are 'new and serious circumstances' that necessitate such data interception. The authorisation should specify the 'precise new and serious circumstances that necessitate and justify a new measure.'[49] The law does not specify a maximum number of extensions. Only the maximum term is fixed (Kerkhofs & Van Linthout, 2013, p. 484).

3.6 Formalities

As far as intrusive surveillance operations are concerned, the law provides that in cases of urgency a decision as referred to in Article 46*quinquies*, paragraph 1 CCP (entering a private place and opening closed objects) may be communicated orally. Afterwards, the decision, with reasons, should be confirmed in writing as quickly as possible.[50]

The authorisation of the investigating judge for the use of data interception should contain the following:[51] 1) indications and concrete facts justifying the measure; 2) reasons why the measure is essential in revealing the truth; 3) the identity of the person, the means of communication, the information system **or** the place which is the object of the measure; 4) the period during which the measure can be exercised; and 5) the name and capacity of the police officers or judicial police officers designated to implement the hacking authorisation.

The authorisation should, in principle, be granted in writing. However, where speed is of the essence the investigating judge may issue the authorisation orally. Article 90*quater*, paragraph 1 CCP provides that the authorisation must be confirmed in writing within 24 hours. The public prosecutor too can issue a data interception warrant (to intercept while the offence is actually being committed). However, the oral warrant must be put in writing as quickly as possible,[52] rather than within the maximum of 24 hours that applies where the warrant is issued by the investigating judge.

Two duties to cooperate are contained in Article 90*quater*, paragraphs 2 and 4 CCP (Royer & Yperman, 2020, p. 32). Paragraph 2 provides that the investigating judge can order the operator of an electronic communication network or providers of electronic communication services (on Belgian territory) to provide (technical) cooperation in order to enable the interception to take place. Kerkhofs and Van Linthout (2019, p. 466) question, among other things, whether an investigating judge will 'still have the energy' to require these parties to cooperate, given the persistent

[48] If allowance is made for the fact that the authorisation does not take effect until the measure is actually implemented, this means that the term for which it is issued may not exceed eight months. The police have a maximum of two months in which to ensure that it is possible to access an automated work.
[49] Article 90*quinquies* CCP.
[50] Article 46*quinquies*, paragraph 1 CCP.
[51] Article 90*quater*, paragraph 1 CCP.
[52] Article 90*ter*, paragraph 5 CCP.

unwillingness to cooperate. In any event, Article 90*quater*, paragraph 2 CCP provides that fines can be imposed on those who fail to cooperate.

Paragraph 4 sets out the second duty to cooperate, namely that the investigating judge can require a person who is suspected of having 'special knowledge', for example about the means of communication, to 'provide information about the operation of the system' and 'about the manner in which access can be obtained in intelligible form to the content of the communication that is being or has been transmitted.' Such a person can also be directed to make the content accessible. A person who refuses to provide technical cooperation is liable to be sentenced to a term of imprisonment of between six months and one year and/or a fine of 26 to 20,000 euros. Royer and Yperman (2020, p. 32) conclude that this duty of cooperation is of only limited value as a general duty of cooperation also exists in Belgium. This is regulated in Article 88*quater* CCP.[53]

3.7 Technical devices

Article 89*ter* CCP contains nothing about the technical devices that can be used in the course of an intrusive surveillance operation. As regards data interception, Article 90*ter*, paragraph 1 CCP provides that technical devices may be installed in computer systems in order to 'decipher and decrypt data stored, processed or transmitted by that system.' The law does not stipulate any specific requirements in respect of the technical devices that can be used.[54] Nor is there any information about this publicly available. According to Kerkhofs and Van Linthout (2019, p. 448), the technologically neutral wording 'technical device' gives the police and the Public Prosecution Service some scope to continue searching creatively for technical tools. As mentioned previously, they believe this would involve installing snooping software or a remote access tool (RAT) (Kerkhofs & Van Linthout, 2019, p. 462). It is apparent from interviews that the police always examine beforehand devices that they may possibly use in order to determine whether they are fit for purpose. The precise criteria that are applied are not public.

3.8 Guarantees

3.8.1 Reliability and integrity of data

Article 90*septies*, paragraph 1 CCP provides that 'suitable means must be used to guarantee the integrity and confidentiality of communications or data from an information system.' According to Kerkhofs and Van Linthout (2019, p. 491), confidentiality concerns the issue of who may consult what data and the manner in which data should be dealt with (for example, whether or not they should be made available to the court registry in sealed form). They indicate that guidelines of this kind

[53] This articles provides for both a general duty to provide information and an active duty of cooperation. The duty to provide information means that there is a duty to 'provide information about the operation of the system or access to it.' The active duty of cooperation means that the person concerned has a duty to 'operate the system himself and to perform certain actions' (Conings, 2020, p. 12).

[54] However, a definition of a technical device has been included. But, as the definition shows, this does not apply to technical devices as referred to in Article 90*ter* CCP. 'A technical device within the meaning of this Code is a configuration of components that detects signals, transports them, activates their registration and registers the signals, with the exception of the technical devices used to implement a measure as referred to in Article 90*ter* (*Parliamentary Proceedings,* House of Representatives 2015-16, no. 54 1966/001, 198).

have been laid down, for example, in Article 90*sexies* CCP and Article 259*bis* of the Penal Code.

According to Kerkhofs and Van Linthout (2019, p. 491), the Belgian legislature has remained very non-committal about the integrity of the data. The legislature merely refers to 'suitable means',[55] but does not explain exactly what is meant by this. It is then up to the defence (during the hearing of the case) to challenge the means that are being used (described in the case file, see later), including the question of whether the evidence that is presented is reliable and sound. Ultimately, this is a matter for the trial judge to decide. Furthermore, the police must provide the best possible explanation, albeit without revealing investigative tactics, of how they obtained certain data and must show that no changes have taken place or could have taken place in the collected data. This could be done by calculating hash values in the case of data that have been seized (Kerkhofs & Van Linthout (2019, pp. 491-492). In one of the interviews, it emerged that the use of hash values is not standard practice. However, ETSI standards are applied (ETSI = European Telecommunications Standards Institute). ETSI plays an important role in supporting legislation and other regulations governing technical (ICT) standards and specifications (ETSI, no date; ETSI, 2020). For example, standards have been formulated for lawful interception (ETSI, no date). Exactly how these standards apply in practice to technical devices used in carrying out data interception has not become clear during this study. Moreover, it emerged during the same interview that, as the police generally exercise a number of investigative powers, the data they collect with the help of the hacking authorisation are not the only evidence.

3.8.2 Reporting

Various other aspects are relevant when it comes to checking the quality of the collected data, namely the manner in which the reporting takes place and the file creation.

In the case of intrusive surveillance operations, the judicial police officer in charge of exercising the power draws up an official report (*proces-verbaal*). This official report is added to the case file no later than when the power ceases to be exercised. If an object has to be removed when the power is exercised (Article 46*quinquies*, paragraph 5 CCP),[56] that should be stated in the official report.[57]

As regards data interception, Article 90*quater*, paragraph 3 CCP provides that judicial police officers must submit a written report on the exercise of the authorisation to the investigating judge at least every five days. Article 90*sexies*, paragraph 1 CCP also specifies what the police should hand to the investigating judge. This is, first of all, a file containing the recorded communication or data.[58] Second, 'the transfer or reproduction of the parts of the recorded communications or data considered by the designated judicial police officers to be important to the investigation', and any

[55] Article 90*septies*, paragraph 1 CCP.
[56] Article 46*quinquies*, paragraph 5 CCP.
[57] Article 46*quinquies*, paragraph 7 CCP.
[58] In practice, this is a DVD burned by the police (NTSU-CTIF). The law provides that a service where the data may be saved (besides the court registry) may be designated by the Crown. This is an additional copy that is kept in order to minimise the possibility of the data being lost. The service concerned should be able to provide sufficient guarantees that recordings are stored in such a way that they remain intact for a longish period and that unauthorised people do not gain access to them (Kerkhofs & Van Linthout, 2019, p. 489). The necessary guarantees should be determined by the Crown (*Parliamentary Proceedings,* House of Representatives 2015-16, no. 54 1966/001, 71).

translation thereof. Third, if relevant, 'the place of the data referred to in the provision in paragraph 2 of the information system' and, fourth, 'a general description of the content and of the identification data of the means of communication or information systems used, as regards the communications or data not deemed important.' Kerkhofs and Van Linthout (2019, p. 482) note that when digital information is intercepted it will not be possible to provide an investigating judge with a substantive update every five days. A large volume of information is generally collected and must first be interpreted. This means that the monitoring by the investigating judge will be somewhat delayed. However, the investigating judge must be given the opportunity, on the basis of the five-day reports, to assess whether the power can continue to be exercised or whether it should be terminated (prematurely). The investigating judge also ultimately decides what selection of data is important for the investigation.[59]

3.8.3 Composition of the file and inspection

The criminal file of a case in which the data interception power has been exercised contains three kinds of documents: 1) the authorisations issued by the investigating judge and any extensions; 2) the five-day reports; and 3) official reports dealing with the actual exercise of the power. These documents must be added to the file no later than when the power ceases to be exercised.[60] The investigating judge decides what selection of data is important for the investigation.[61] There are no procedural rules governing how data should be selected (Kerkhofs & Van Linthout, 2019, p. 483). As regards the mentioning of names of persons who are involved in one way or another in the interception, Kerkhofs and Van Linthout (2019, p. 480) state that the legislature is not clear about what names should or should not be mentioned. The explanatory memorandum to the legislation states that the names of support staff, such as the administrative and logistics support staff (see the section on competent authorities), need not be mentioned. However,[62] the law states that only the names of the persons involved with the actual hacking need not be mentioned in the case file. Kerkhofs and Van Linthout (2019, p. 480) submit that it therefore follows that the names of persons other than the hackers should be mentioned. Only in this way can the investigating judge determine whether a highly privacy-invasive measure such as data interception[63] 'remains under control' and that 'not just anyone' can acquaint themselves with the data collected through the exercise of that power. According to Kerkhofs and Van Linthout (2019, 480), it is apparent from the explanatory memorandum to the Bill to protect privacy from measures to listen to, take note of and record private communications and telecommunication (*Parliamentary Proceedings,* Senate 1992-93, 843-1, 16) that limiting the number of people involved in the implementation provides an 'additional guarantee of confidentiality'. As they go on to note (2019, p. 480), however, this is not regulated in that way in Article 3 of the Royal Decree of 17 October 2018. In their view, it is apparent from that article that direct checks are no longer carried out by the investigating judge, only by the police themselves.

All documents that have been used in the investigation but not added to the case file are either destroyed or sent to the court registry. Kerkhofs and Van Linthout

[59] Article 90*sexies*, paragraph 2 CCP.
[60] Article 90*sexies*, paragraph 4 CCP. This has not been regulated in this way for Article 89*ter* CCP. In such cases, the case file only contains the authorisation and the official report of the exercise of the power and any further official reports concerning what may or may not have been found and/or analysed (personal communication, 24 March 2023).
[61] Article 90*sexies*, paragraph 2 CCP.
[62] Article 90*quater*, paragraph 3 CCP.
[63] Article 90*ter* CCP.

(2019, p. 488) wonder whether a sufficient check can be made in this situation. After all, only a small selection of documents ultimately end up in the case file. This concerns the following documents: 'Every note [which is made] in the course of implementing the measures referred to in Articles 90*ter*, 90*quater* and 90*quinquies* by the persons designated for this purpose (...).'[64] Article 90*septies*, paragraph 4 CCP specifies what documents (already listed at the start of this section) are kept in a sealed container at the court registry.

Data that are intercepted on the basis of Article 90*ter* CCP need no longer be fully transcribed. It is sufficient to include a selection of them in the file. However, the scope for oversight of that selection has been increased. Article 90*septies*, paragraph 6 (1) CCP provides that 'the accused, the civil party or their counsel' should, on request, receive a copy of the recorded data, some of which are in the official report. A situation may occur in which the requesting party, for example counsel, wishes to have the data he/she has requested added to the case file. In such a case, a request must be made to the investigating judge. If counsel submits a request to the investigating judge, the latter will process the request in accordance with Article 61*quinquies* CCP, as is apparent from Article 90*septies*, paragraph 6 CCP. The latter article also gives three reasons why a judge may reject the request: 1) if he/she does not consider the additions to be necessary in order to reveal the truth; 2) if he/she considers that the addition would at that time be detrimental to the investigation; and 3) on account of the need to protect other rights or interests of persons.

Under the legislation on pre-trial detention, an accused is provided with information about the preliminary judicial investigation once he/she has been arrested. This may mean that an accused also obtains information about the current exercise of investigative powers, such as data interception, for example in relation to other accused persons. It is to prevent such a situation that Article 90*sexies*, paragraph 4 CCP has been introduced. This provides that authorisations issued by the investigating judge, reports of judicial police officers and official reports relating to the exercise of a power should be added to the case file no later than the date on which the power ceases to be exercised (Kerkhofs & Van Linthout, 2019, p. 490

3.8.4 The duty of notification

Article 90*novies* CCP provides that every person in respect of whom the power of data interception (Article 90*ter* CCP) has been exercised must be notified in writing of the nature of the exercise of that power and the days on which it was exercised.[65] No later than fifteen days after the decision on the manner in which the administration of justice is regulated has become final and after the writ of summons as referred to in Article 524*bis*, paragraph 6 CCP has been deposited at the registry of the district court or the court of appeal, the registry will notify the person in respect of whom the power has been exercised. The registrar does this in response to an application from the public prosecutor or, when the occasion arises, from the Procurator General. An exception to the duty of notification exists in cases where it is not reasonably possible to discover the identity or place of residence of the person concerned.

[64] Article 90*septies*, paragraph 3 CCP.
[65] This condition is not prescribed on pain of nullity and is not always applied equally strictly (personal communication, 24 March 2023).

3.8.5 *External oversight*

Besides the oversight by the judicial authorities, Belgium has a standing committee for oversight of the police services (*Vast Comité van Toezicht op de politiediensten*, known as 'Committee P'). This committee was introduced in the 'Law regulating oversight of police and intelligence services and of the Organisation for the coordination of the threat assessment' of 18 July 1991 (referred to below as the Police Oversight Law). Committee P is an 'external institution which is charged, under the supervision of the Federal Parliament, with oversight of the overall operation of the police, inspection and enforcement services' (Committee P, no date). Committee P is not responsible for oversight of judicial authorities or the acts they perform in relation to prosecutions or for oversight of administrative acts by the police authorities.[66] However, Committee P does monitor 'the exercise of police duties by all competent officials'. It also monitors how 'fundamental rights and freedoms are observed and actively promoted' (Committee P, no date). Committee P also prepares annual reports and special articles. As far as is known, the annual reports and articles published by Committee P do not contain any information about the use of data interception and intrusive surveillance. Nor are there any indications that the Committee intends to focus on this in the near future.

3.9 Case law

Article 90*decies* CCP provides that the Minister of Justice should publish an annual report on Articles 90*ter* to 90*novies* inclusive. Parliament should be kept informed about the number of investigations instituted under these articles, the duration of the measures taken, the number of persons involved and the results achieved. This report is not made public. Moreover, on the basis of this report it is not really possible to discover how often Article 90*ter* has been used. After all, Article 90*ter* CCP also covers 'ordinary' telephone taps. As far as is known, it seems from the available case law that police hacking is seldom challenged in court (personal communication, 24 March 2023). One of the interviewees indicates that this concerns the way in which the hack took place.

3.10 Conclusion

Belgium has two statutory provisions which permit the police to access a computer system: Article 89*ter* CCP and Article 90*ter* CCP. Under Article 89*ter* CCP, a special team of the Belgian police may search a computer system and take a 'sample' of the data ('intrusive surveillance operation'). Under Article 90*ter* CCP, the police may gain entry to a computer system and gather data from it (data interception). Using the second of these powers, the police can collect much more information than by mounting an intrusive surveillance operation.

Little is contained in the law about technical devices and any requirements they must satisfy, for example relating to the quality of the data. One of the few things mentioned is that a technical device may be used. The only provision concerning the criteria that a technical device must fulfil is that suitable steps must be taken to guarantee the integrity and confidentiality of the collected data. What exactly should be understood by 'suitable' is not made clear. The same applies to the question of who

[66] Article 2, Police Oversight Law.

should check this suitability. In practice, the police themselves test the technical devices. In addition, as the police tend to exercise two or more powers simultaneously, the case file is not dependent solely on data gathered by data interception.

Unlike the situation before the exercise of the power, the position is rather better regulated in Belgium with regard to the use of technical devices during the exercise of the power and above all after the end of its exercise. A number of conditions apply to the confidentiality of data, for example with regard to who may consult data, where they are stored (in a registry) and who may subsequently have access to them. This means that, in theory, not just anyone can access the collected data. As the legislation on this is not unequivocal, there are only limited checks on who has gained access to the data. Responsibility for such checks rests not with the investigating judge but with the police themselves. Another form of check is the five-day reports that have to be submitted to the investigating judge. This means that an independent party checks implementation. Incidentally, the checks will always lag behind the progress made by the actual investigation because processing the large volume of data collected is very time-consuming. Finally, the main possibility of a check is built in after the data have been collected and the accused and the defence gain access to the case file and the matter comes before a judge. On the basis of the file, the defence can raise questions designed to query whether the means employed were suitable. However, it is debatable how much information about this will be disclosed as no statements are generally made about the exact operation of a technical device. Moreover, not all data are automatically added to the case file. Nonetheless, the defence can, subject to certain conditions, get an idea of the collected data and whether they are complete and may request that data be added to the file.

4 Germany[67]

Special thanks to Rainer Franosch (Ministry of Justice, Germany) for critically reading this chapter for factual inaccuracies.

4.1 Statutory regulation

On 24 August 2017, a law came into force in Germany to give a more effective and practical approach to criminal law enforcement (‘*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*‘) (Bundesministerium der Justiz, n.d.). Among other things, this law amended the German Code of Criminal Procedure (‘*Strafprozeßordnung*’), hereinafter CCP. It created two hacking possibilities for investigative authorities for the purpose of investigating and prosecuting criminal offences (Škorvánek, Koops, Newell, & Roberts, 2020, pp. 1012-1013).[68] Based on the amendments, the police may intercept telecommunications at the source (‘*Quellen-Telekommunikationsüberwachung*’),[69] hereinafter source interception, and conduct online searches in an information technology system (‘*Online-Durchsuchung*’),[70] hereinafter computer system.[71]

Splitting the source interception and the online search stems from the decision of the Federal Constitutional Court, the ‘*Bundesverfassungsgericht*’, hereinafter BVerfG,[72] from 2008 (Bundesverfassungsgericht, n.d.) (Škorvánek et al., 2020, p. 1013). The BVerfG passed judgment on a North Rhine-Westphalia law allowing investigative authorities in that federal state to covertly search suspects’ computers via remote access (Groothuis, 2008, p. 990). The BVerfG declared the online search null and void and judged that the use of the power was incompatible with Article 2(1) of the German Constitution in conjunction with Article 1(1), Article 10(1) and Article 19(1), second sentence, of the German Constitution.[73] This decision led, among others things, to the inclusion of the right to protect the confidentiality and integrity of information technology systems into the right of personality (‘*allgeMayne Persönlichkeitsrecht*’)[74] (Groothuis, 2008, p. 990). The more extensive a power infringes on an individual’s private life, the more restrictive the conditions must be for its use (Deutscher

67 Germany has different ways of referring to legal provisions. For purposes of readability, the decision has been made to use the Dutch method of referral here.

68 The German federal police may also be authorised for preventive hacking based on the ‘*Bundeskriminalamtgesetz*’ (BKAG). The legal basis for source interception is laid down in Section 51(2) of the BKAG and the legal basis for the online search is laid down in Section 49 of the BKAG. The BKAG sets out the duties and powers of the German federal police, which primarily deal with criminal offences such as terrorism and human trafficking (Fedorova, Te Molder, Dubelaar, Lestrade, & Walree, 2022, p. 128). Some federal states (‘*Bundesländer*’) have also laid down a preventive hacking power in their police acts (Škorvánek et al., 2020, p. 1012). This report limits itself to the discussion of the two possibilities set out in the Code of Criminal Procedure.

69 Section 100a(1), second and third sentence, CCP.

70 Section 100b(1) CCP.

71 Source interception is directed at communications, while online searches are aimed at data. For a more comprehensive description, see Sections 4.1.1 and 4.2.2.

72 The BVerfG is the highest Court in Germany which determines whether laws are constitutional. The BVerfG can also rule in criminal cases in the event of a (possible) violation of the Constitution (Klip, Peristeridou, & De Vocht, 2019, p. 35).

73 Section 2(1) of the German Constitution in conjunction with Section 1(1) of the German Constitution governs the personality right, in relation with the fundamental right of human dignity. Section 10(1) of the German Constitution comprises the telecommunications confidentiality and Section 19(1) of the German Constitution covers the restriction of fundamental rights (also see Groothuis, 2008, pp. 990-991).

74 The personality right implies that every individual may develop his or her personality (Section 2(1)of the German Constitution in conjunction with Section 1(1) of the German Constitution).

Bundestags, 2017, p. 47).[75] Online searches allow investigative authorities to create a detailed personality profile of citizens (Groothuis, 2008, p. 1001). This profile is more detailed in online searches than it is in intercepting telecommunications. The latter only infringes the telecommunications confidentiality set out in Section 10 of the German Constitution, on which less demanding safeguards are imposed. Given that the extent to which the powers infringe on privacy varies, the powers are covered in two separate statutory provisions (Škorvánek et al., 2020, p. 1013).

4.1.1 Source interception of telecommunications

The existing power to intercept telecommunications as set out in Section 100a CCP was expanded in 2017 with an additional provision enabling source interception. See the second and third sentence of Paragraph 1. Before 2017, investigative authorities could already intercept communications, such as telephone conversations, fax messages and emails, without the knowledge of the suspect, based on the former Section 100a CCP (‘*Telekommunikationsüberwachung*’). The assistance of telecommunications companies and internet service providers was needed to undertake this power (Niedernhuber, 2017, p. 170). However, this traditional power could not retrieve the contents of encrypted communications. The new provision does allow for this (Deutscher Bundestags, 2017, p. 49). Based on the newly-introduced Section 100a CCP, investigative authorities may, with the use of a technical tool, interfere with a suspect’s computer system, such as a laptop, a tablet or a mobile phone (Niedernhuber, 2017, p. 170). Hacking into a computer system ensures that before communications are encrypted or after communications are decrypted, the police can read and record those communications ‘at the source’.[76] In terms of telecommunications, this includes Skype conversations and messages sent via messenger services such as WhatsApp and Telegram (Niedernhuber, 2017, p. 170; Singelnstein & Derin, 2017, p. 2647).[77] Investigative authorities are not allowed to switch on cameras or microphones, or change data (Niedernhuber, 2017, p. 172). However, investigative authorities may intercept and record the content and circumstances of the communications, stored in the suspect’s computer system. These are stored data related to telecommunications from the past (Škorvánek et al., 2020, p. 1014), including metadata. A prerequisite in this context is that investigative authorities must also have been able to intercept and record these data in encrypted form during the transmission processes in the public telecommunications network.[78] This is a key difference from the online search (see next section). Source interception only allows for the interception of communications present at the time when an order has been issued (Deutscher Bundestags, 2017, p. 50).

4.1.2 Online search

The second power permitting investigative authorities the opportunity to hack is the online search. Based on Section 100b(1) CCP, investigative authorities may, with the use of a technical tool, covertly gain access to and extract data from a suspect’s computer system. In principle, investigative authorities gain access to all data stored on the suspect’s computer system. They can also read all messages sent before the authorisation was given for the online search (Deutscher Bundestags, 2017, p. 50; Niedernhuber, 2017, p. 171). In view of the terminology used in the legal text, which

[75] This is also known for the 'Kernbereich privater Lebensgestaltung' concept (Lindemann & Van Toor, 2018).
[76] Section 100a(1), second sentence, CCP.
[77] There is a debate in academic literature on what else is meant by telecommunications. See, for example: Niedernhuber (2017) and Singelnstein and Derin (2017).
[78] Section 100a(1), third sentence, CCP.

refers to the extraction of stored data from a computer system, several authors conclude that investigative authorities may not activate the camera or microphone of the suspect's computer system in order to make video or audio recordings (Lindemann & Van Toor, 2018, p. 381; Niedernhuber, 2017, p. 172; Singelnstein & Derin, 2017, p. 2647). Investigative authorities are also not allowed to modify stored data (Niedernhuber, 2017, p. 172; Singelnstein & Derin, 2017, p. 2647). Moreover, the deployment of the power must be limited to the data relevant to the criminal proceedings in question. An extensive investigation of the entire computer system is unacceptable (Singelnstein and Derin, 2017, p. 2647).

The law does not define the exact means by which investigative authorities can hack into a computer system. They need to do this by means of technical tools or via a '*kriminalistischer List'*, e.g social engineering. Furthermore, there is no legal basis for investigative authorities to covertly enter a physical place, such as a suspect's home, to then hack into their computer system (Deutscher Bundestags, 2017, p. 52).

4.2 Competent authorities

The execution of the source interception and online search takes place at the '*Bundeskriminalamt'*, the German federal police, hereinafter BKA (Deutscher Bundestags, 2017, p. 52). In principle, any competent police authority may exercise these powers. In practice, not all police units have the right resources. The public prosecutor decides which police department will carry out the powers (personal communication, 23 May 2023). An interview shows that, in practice, the forensics team of the police carries out the source interception and the online search. Other investigative teams can contact this team for the deployment of both powers.

Both powers require a form of judicial review, as described in Section 100e CCP. In the case of source interception, an investigating judge has to authorise the use of the power (court order), following a request from the Public Prosecution Service. In exigent circumstances, the Public Prosecution Service may issue an order directly, i.e. without the court's prior permission. However, the deployment of that power will need to be approved by a court judge within three working days.[79] In the case of online searches, the Public Prosecution Service submits a request to the *'Kammer des Landgerichts',*[80] which must approve a possible deployment.[81] This involves a '*Staatsschutz'* division of a regional court, consisting of three judges (Soiné, 2018, p. 496).[82] The fact that a chamber decides on the deployment means that, unlike in the case of source interception, multiple judges are involved in the authorisation of the online search, as evidenced by some interviews. In exigent circumstances, the president of the division ('*Vorsitzenden'*) may grant an order. The regional court will then still need to approve the power within three working days.

79 Section 100e(1) CCP.
80 The *'Landgericht'* in the district where the Public Prosecution Service is located is the competent court to grant authorisation for the deployment of the power specified in Section 74a(4) of the '*Gerichtsverfassungsgesetzes'* (Section 100e(2) CCP).
81 Section 100e(2) CCP.
82 The judiciary in Germany has the following set-up: local judicial authority ('*Amtsgerichte'*), regional judicial authority ('*Landgerichte'*), higher regional judicial authority ('*Oberlandesgerichte'*) and the federal judicial authority ('*Bundesgerichtshof*'). The latter is the highest authority in the federal judiciary (Struijk, 2018, p.496).

4.3 Against whom?

In principle, the deployment of both powers has to be done in a targeted manner. The source interception must pertain to the communications of a suspect. The police may also intercept communications from persons from whom it can be assumed, on the basis of certain facts, that they receive or send messages intended for or originating from the suspect. Furthermore, this power may be deployed in respect of another person's telephone connection or computer system used by the suspect.[83] In principle, online searches also target a suspect. Additionally, investigative authorities may interfere with other persons' systems, provided that there are certain facts based on which it can be assumed that the suspect is using those other persons' computer systems and if interference into the suspect's computer system does not lead to the establishment of the facts or to the determination of the whereabouts of a fellow suspect.[84]

4.4 Cases

The source interception of telecommunications is permissible if there is a suspicion that the suspect, either as offender or participant, has committed a serious criminal offence (*'schwere Straftat'*). These serious criminal offences are listed in Section 100a(2) CCP. They include e.g. extortion, drug-related criminal offences and money laundering. Investigative authorities may also intercept telecommunications in the event of an attempt of or preparation for a serious criminal offence.[85] For an online search, there needs to be a suspicion that the suspect, either as offender or participant, has committed a very serious criminal offence (*'besonders schwere Straftat'*). Section 100b(2) CCP lists these types of criminal offences, e.g. organised crime, aggravated murder and human trafficking. Online searches are also allowed in the event of an attempt of or preparation for a very serious criminal offence.[86]

4.5 Term of authorisation

Source interception can be authorised for a maximum period of three months. The deployment of the power may each time be extended by three months. This is only allowed if, taking into account the information gathered in the course of the investigation, the prerequisites of the original authorisation for source interception still apply.[87] The law does not specify a maximum period of time for the deployment of this power. The same applies to the maximum number of extensions.
An online search may be deployed for a maximum period of one month. The authorisation for the deployment of the power may each time be extended by one month, to a maximum initial period of six months. If the six-month period is met, the *'Oberlandesgericht',* a higher regional court than the *'Landgerichte'* (Škorvánek et al., 2020, p. 1015; Struijk, 2018, p. 496), will then decide on any further extension orders. The law does not specify a maximum number of extensions or a maximum period of time. Also for online searches, the prerequisites of the original authorisation

83 Section 100a(3) CCP.
84 Section 100b(3) CCP.
85 Section 100a(1) under 1, CCP.
86 Section 100b(1) under 1, CCP.
87 Section 100e(1) CCP.

must continue to apply, taking into account the information gathered in the course of the investigation.[88]

4.6 Formalities

The judge or court deciding on the deployment of the power, or its extension, substantiates the requirements and main considerations subject to its decision. The judge or court must specifically state the following in each individual case: the particular facts on which the suspicion is based and the main considerations regarding the necessity and proportionality of the deployment of the power.[89] At any time the conditions for deployment can no longer be met, the deployment of the power is terminated immediately. The court will be informed accordingly.[90] Furthermore, the authorisation from the judge or court must be granted in writing.[91] The written authorisation has to include the following:

1 To the extent known, the name and address of the suspect to whom the power is directed.
2 The alleged criminal offence.
3 The type, extent, duration and the end date of the deployment of the power.
4 The type of information that has to be collected and its relevance to the investigation.
5 As precise as possible a description of the computer system from which data are to be collected when it comes to the deployment of the power set out in Section 100a(1), second and third sentence, CCP or Section 100b CCP.[92]

In addition to the suspicion that the suspect has committed a serious or very serious criminal offence, the deployment of both powers is only permitted if the criminal offence is one of particular severity in the individual case as well.[93] Also, other measures for establishing the facts or determining the whereabouts of the suspect must have no or less chance of success, i.e. the principle of subsidiarity (Lindemann & Van Toor, 2018, p. 381).[94] In case of the source interception, this means, for example, that the deployment of this power is only admissible once the traditional power of interception cannot be used (Singelnstein & Derin, 2017, p. 2648).

Finally, investigative authorities must take into consideration the suspect's core area of private life (*'Kernbereich privater Lebensgestaltung'*). Section 100d CCP states that the source interception and online search are inadmissible if there are any indications for assuming that the deployment of such powers will only result in findings in the core area of a suspect's private life. If such findings are made during the deployment of either power, recordings of such findings must be deleted immediately. Moreover, when deploying an online search, technical measures must be taken to ensure that any data from a suspect's private life cannot be captured.[95]

88 Section 100e(2) CCP.
89 Section 100e(4) CCP.
90 Section 100e(5) CCP.
91 Section 100e(3) CCP.
92 Section 100e(3) CCP.
93 Lindeman and Van Toor (2018, p. 381) give the example of a forced French kiss which can be punished as rape. Rape is a serious crime, but it could be said that some acts that can be qualified as rape will not be seen as a serious crime in practice.
94 Section 100a(1) and Section 100b(1) CCP.
95 Refer to Section 100d(1)(2)(3) CCP.

4.7 Technical tools

Both Section 100a(1) CCP as well as Section 100b(1) CCP stipulate that investigative authorities may make use of technical tools. For source interception, the BKA has developed in-house software and has commercial software at its disposal as well. This software is not released until it has passed an extensive test procedure and once it has been established that the software meets the statutory requirements and the SLB guideline (‘*Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung*’). The SLB guideline formulates objectives and measures that the software to be used must comply with. The software also undergoes continuous development, depending on operational requirements. The BKA also has software for online searches (BKA, n.d.). It is unclear whether this includes both software developed in-house and commercial software.

In principle, all technical aids may be used as long as they meet the legal and constitutional requirements.[96] In practice, the police will have to ensure that the means used meet the conditions. The SLB guideline is an internal guideline for investigative officers and has no further binding legal status (personal communication, May 23, 2023). The first SLB guideline was drawn up in 2012 by the security authorities of both the federal government and the federal states. On 2 October 2012, two working groups of the Confederation of Ministers of the Interior (‘*Innenministerkonferenz*’) took cognisance of the proposed guideline. They recommended both the federal government and the federal states to use this guideline as a basis for the procurement and development of interception software. The 2012 guideline was amended because of the short innovation cycles that modern information technology systems and their software typically have, and because the German Code of Criminal Procedure was amended in 2017 (BKA, 2018, p. 1). The original guideline, which focused on interception and PC platforms, contained some highly specific technical specifications. The latest version of the guideline is worded in a more open manner. This means that instead of specifying techniques, it specifies objectives to be achieved. Moreover, the guideline not only applies to source interception, it also includes online searches (BKA, n.d.). The aim is to update the guideline regularly. The most recent version is dated 5 October 2018 (BKA, 2018). The guideline shows that the software used for both powers consists of a number of components that function as one single system:

1 The extraction software (‘*Ausleitungssoftware*’) is installed on the suspect’s computer system and ensures that data are collected and transmitted to those executing the power.
2 The registration and control unit (‘*Steuer- und Aufzeichnungseinheit*’) is used by executive actors to control the extraction software, to record the data from the court decision and to log all activities.
3 The network connection (‘*Netzwerkverbindung*’) transfers the communications of the suspect’s computer system to the registration and control unit of the investigative authorities, and back again (BKA, 2018, p. 2).

[96] The legal terms can be found in §100a (5). The constitutional conditions follow from case law of the Federal Constitutional Court (BVerfG, Urteil vom 27. 2. 2008 – 1 BvR 370/07, 1 BvR 595/07). Secret infiltration of an automated work must always be based on a court order and a law that allows intrusion must contain provisions to protect privacy (personal communication, June 7, 2023).

4.7.1 ZITiS

Since 2017, Germany has an organisation that can provide support to investigative authorities with market survey and the development of technical tools for the source interception and online search. This organisation, called '*Zentrale Stelle für Informationstechnik im Sicherheitsbereich'*, hereinafter: ZITiS, falls under the responsibility of the German Ministry of the Interior and Community, but has no investigative powers and is not involved in the use of technical tools.[97] ZITiS's task is to support and advise federal security services on information technology security tasks. It also has a role in relation to products such as technical tools for federal security services, research into these and their development.[98] One interview shows that ZITiS can, for example, conduct a market survey at the police's request, e.g. which technical tools are available on the market and what is their quality. ZITiS also assesses whether technical tools for source interception or online searches comply with German legislation. While from a legal point of view the recommendations of ZITiS do not constitute a certification, they can help the police in purchasing technical tools. The final decision on the purchase of technical tools is made by the investigative team, and it is that team that has to purchase the technical tool. The final decision on the purchase of a technical tools lies with the police and purchase the tools themselves. ZITiS also recently started developing its own technical tools for the hacking power, as evidenced by an interview.

4.8 Safeguards

4.8.1 Technical requirements

Although the law, as far as is known, does not stipulate anything about the type of technical tools investigative authorities may use, it does set out a number of requirements that a technical tool must meet. These requirements apply to both source interception and online searches. Section 100a(5) CCP sets out the requirements that technical tools must meet for the source interception. The requirements are as follows:

1 A technical tool should be installed in such a way that it only records ongoing communications[99] or the contents and circumstances of the communications.[100]
2 Technical tools may only make modifications to the relevant person's computer system that are essential to the data collection.
3 If technically feasible, the modifications made to the computer system must be automatically reversed after the deployment of the power has ended.
4 Furthermore, technical tools must protect against unauthorised use by third parties, according to the state-of-the-art. Copied data must be protected against any modification, unauthorised deletion and unauthorised access by third parties, according to the state-of-the-art.

Section 100b(4) CCP stipulates that these requirements also apply to technical tools used for an online search, with the exception of the first requirement.

97 Section 1 from the ZITiS Implementation Decision, the '*Erlass über die Errichtung der Zentralen Stelle für Informationstechniek im Sicherheitsbereich*', hereinafter: Implementation Decision (Bundesministerium des Innern, 2017).
98 Section 2 of the Implementation Decision. See also: Zitis (n.d.).
99 Section 100a(1), second sentence, CCP.
100 Section 100a(1), third sentence, CCP.

In addition to these statutory requirements, the SLB guideline contains various aspects intended to ensure that the development, procurement and use of the software takes place within an uniform framework (BKA, 2018). The topics included in the guideline are largely related to the requirements set out in the law. The guideline is structured into the following topics: protection targets and security measures, work processes and procedures, suppliers, and test policy. The guideline also presents a framework based on which the development and the use of software is considered. This involves risk analyses and IT security concepts. According to the SLB guideline, special security concepts need to be developed in order to deploy both powers, i.e. source interception and online searches. Both software suppliers and the users of the software must conform to these concepts. Part of an IT security concept is performing a risk analysis. Such an analysis must, among other things, cover threats that may affect the IT process and existing residual risks. Objects at risk, e.g. system components such as hardware and software, applications, organisational or personnel issues, must be described and evaluated. The results of the risk analysis, the determination of the protection needs and the resulting consequences and implementation thereof are laid down in the IT security concept. This security concept has to include appropriate, state-of-the-art security measures (BKA, 2018, p. 4).

Protection targets and security measures
The SLB guideline mentions the following protection targets: confidentiality, integrity/authenticity, and availability of data. Reliability means that no unauthorised access takes place. Integrity and authenticity are understood to mean that collected data are protected from modifications and that data modifications are traceable. The transfer of communications may only take place between the extracting software on the suspect's computer system and the registration and control unit of the executing authority. Finally, availability means that measures must be taken to prevent the loss of extracted data and to protect the entire computer system from failures (BKA, 2018, p. 3). The guideline notes that it requires state-of-the-art (technological) measures to achieve these targets. Such measures include for example the use of cryptographic methods (BKA, 2018, pp. 3-4).

Work processes and procedures
The execution of both powers is performed in accordance with the statutory and organisational frameworks as well as with the concepts for organisational processes and quality assurance jointly developed by the federal and federal-state security authorities. The objective is to create overarching standards that ensure the best possible execution of both powers and minimise the risk of discovery. This is expected to ensure standardised and legitimate use of software (BKA, 2018, p. 5).

The formulated processes and procedures pertain to the following themes: the scope of access to data as referred to in the order, access rights and role assignment, and modifications to the suspect's computer system. They also pertain to the protection of third parties who are not directly involved in the investigation, updates, and protection from disclosure and traceability.

Scope of access to data and roles and rights
In terms of access to collected data, appropriate technical and organisational security measures must be taken to ensure that the person exercising the power can only access the content covered by the order. This must be registered or documented. This specifically serves to protect the right to privacy. The processes are in accordance with the relevant statutory frameworks (BKA, 2018, p. 5).

The guideline further states that roles and access rights must be defined in such a way that users only have access rights needed to perform their role. This means that access protection has to be safeguarded in line with data protection legislation, related registration and, in particular, compliance with privacy regulations. The executing authority is responsible for the concrete implementation of the access rights and roles concept in accordance with the organisational and legal prerequisites (BKA, 2018, p. 5).

Modifications to the suspect's computer system
With regard to modifying the suspect's computer system, the guideline states that the computer system may not be affected more than necessary. Security measures protecting the suspect's computer system from outside access are also not intended to be restricted for longer than necessary. In addition, security measures must protect the interface, by means of which the extraction software makes data available to users, against unauthorised use. Prior to the use of the software, it is necessary to verify and document that the software's interference with the suspect's computer system is kept to the unavoidable minimum (BKA, 2018, p. 5).

The software must be removed immediately after the data collection has been completed. If there have been any modifications to the suspect's computer system during the exercise of the power, these must be restored to the extent that is technically possible. This requires the software to have appropriate features so that recovery is feasible even if the suspect's computer system is no longer accessible by the registration and control unit (BKA, 2018, p. 6).

The protection of third parties and updates
The extraction software may only be used for the computer system mentioned in the order. It is therefore important to identify this computer system as accurately as possible. If the extraction software is installed on a computer system other than the suspect's computer system, care must be taken to ensure that no data from that computer system are transferred other than the data required in the context of identifying the suspect's computer system. Also, to the extent that this is technically possible, the software must be removed immediately and any changes made must be restored (BKA, 2018, p. 6).

Updates are subject to specifications and measures that ensure the reliability, integrity/authenticity, and traceability of data. This ensures that updates to the software are made only via the executing authority's registration and control unit. Logging and documentation must make it possible to track what updates have been carried out and when. As far as this is technically possible, appropriate security measures must rule out discovery and traceability to the executing authority. In particular, the software must be protected against reverse engineering. Should any security issues arise with the software or with the registration and control unit, the software provider is obliged to promptly fix these issues and provide appropriate updates. Executing authorities must install these updates without delay, in accordance with the IT security concept (BKA, 2018, pp. 6-7).

Traceability
The guideline emphasises the importance of the data's traceability and authenticity. Since data are used for law enforcement and security purposes, it is imperative that full insight can be given into the collection, evaluation and further processing of the data by the executing authority.

Logging and documentation must ensure that the lawfulness of the data collection and the way data have been processed can be verified. Logging and documentation must ensure the protection of fundamental rights, but also the integrity (usability in court cases) of the data extracted. Furthermore, documentation above all helps to prove that data actually originate from the suspect's computer system, that they are complete and that they have not been manipulated. The software used has to be archived to ensure traceability. The duration of the storage of protocol data depends on the legal requirements of the federal government and the different federal states.

Software suppliers
The guideline states that suppliers ('*Anbieter*') of software have to undergo a careful selection procedure. For domestic suppliers, the German Federal Ministry for Economic Affairs and Technology would have to draw up a security report. An appropriate procedure has to be sought for foreign suppliers (BKA, 2018, p. 7). Suppliers have to guarantee that they will comply with the conditions and prerequisites stemming from the legal framework and the SLB-guideline. They also have to ensure the following:

1 They act in line with state-of-the-art secure software development.
2 Only authorised persons have physical access, access to logging and access to the development environment.
3 External components such as software libraries[101] are purchased from verified sources and tested before use as to their security properties.
4 Authorities using the software are immediately notified of any security incidents, identified security deficiencies or other events that compromise the secure, legal and proper execution of powers.

Authorities using the software or other authorities designated thereto assess these aspects, for example as part of a tendering procedure (BKA, 2018, pp. 7-8).

Testing and purchase
Software approval is based on a defined test procedure, the results of which are recorded as part of the overall acceptance process. Prior to each application, the executing authority tests whether the legal requirements have been met in the specific case, for example in terms of the software features used. The results of this test are documented (BKA, 2018, p. 8). Furthermore, one of the interviews shows that sometimes independent organisations, such as TÜV and the Fraunhofer-Gesellschaft, can also be asked to inspect technical tools.[102] Their exact role has not become clear in this study.

4.8.2 Reporting and file

In addition to the measures just mentioned, there are other measures relevant to the quality and the control of the quality of the data collected, such as the manner of reporting, dossier formation and the notification obligation.

Each time a technical tool is used for source interception or an online search, investigative authorities must draw up a report on this.[103,104] This is a logging obligation which can be used to check whether investigative authorities have used the

[101] A software library is a suite of data and programming code that is used to develop software programs and applications (Techopedia, 2016).
[102] Two media reports also mention the role of TÜV (Meister, 2018; Flade, 2018).
[103] Section 100a(6) CCP.
[104] Section 100b(4) CCP.

power lawfully. The report has to provide the following information: 1) the name of the technical tool and the time of its use; 2) information about the identification of the computer system and non-temporary modifications to it; 3) information based on which the collected data can be recorded; and 4) the unit executing the power.[105] In addition to reporting on the use of the technical tool, the Public Prosecution Service must keep a record of all decisions and documentation relating to the online search. This information is added to the file as soon as the notification obligation has been met.[106] Other rules apply to personal data (*'Personenbezogene Daten'*).[107]

Based on Section 101(4) CCP, persons in respect of whom either source interception or an online search has been deployed need to be informed that investigative authorities have deployed these powers. That notification has to take place as soon as possible. Notifications may be deferred, for example if the purpose of the investigation and/or the life, the physical integrity and the personal freedom of a person or significant assets would otherwise be in jeopardy.[108] If notification is deferred and does not take place within twelve months of completion of the deployment of the power, the competent court will decide on any further deferment and its duration. The competent court may also decide that notification is to be omitted altogether.[109]

4.9 Case law

Each year, the federal states and the Procurator General (*'Generalbundesanwalt'*) must submit a report to the Federal Office of Justice (*'Bundesamt für Justiz'*) on the deployment of the interception of telecommunications, the source interception of telecommunications and online search. The Federal Office of Justice creates a nationwide overview of these reports and publishes them online.[110] The annual overview must contain the following information about both powers:

1 The number of cases in which the order under Section 100a(1) CCP (traditional power to intercept telecommunications) or Section 100b(1) CCP has been issued.
2 The number of orders. A distinction is made between initial and follow-up orders.
3 The underlying criminal offence based on which the power had been deployed.
4 The number of cases in which an interception of the computer system under Section 100a(1), second and third sentence, CCP (source interception) has been ordered and has been actually executed. In the case of online searches, the number of cases in which interference with the suspect's computer system has actually been carried out.[111]

In 2020, source interception was executed fourteen times. The online search was ultimately executed eight times in 2020 (Bundesamt für Justiz, n.d.).

As far as is known, based on the interviews conducted, there is currently no case law available from court cases in which the deployment of the hacking power has been raised with regards to the quality of the data acquired.

105 Section 100a(6) CCP.
106 Section 101(2) CCP.
107 Section 101(3)(8) CCP.
108 Section 101(5) CCP.
109 Section 101(6)(7) CCP.
110 Section 101b(1) CCP. See Zie Bundesambt für Justiz (n.d.).
111 Section 101b(2)(3) CCP.

4.10 In conclusion

In Germany, investigative authorities may hack based on two legal provisions. The source interception referred to in Section 100a(1), second and third sentence, CCP allows investigative authorities to intercept telecommunications at the source. The online search described in Section 100b(1) CCP allows investigative authorities to gain access to, in principle, all data stored in a suspect's computer system. With this second power, investigative authorities make a more intrusive infringement on the private lives of suspects, which is why stricter conditions apply to the deployment of an online search. Based on the two aforementioned legal provisions, investigative authorities may not activate any cameras or microphones to make video or audio recordings. Nor are they allowed to make any modifications to data.

Technical tools may be used for the deployment of source interception and online searches. The German Code of Criminal Procedure includes certain safeguards to ensure the quality of the data collected as much as possible. The SLB guideline drawn up by the security authorities also describes a number of safeguards, partly overlapping with the legal requirements. Incidentally, this guideline (deliberately) does not specify how these safeguards should be realised in practice. The SLB guideline applies to both tools developed in-house as well as software created by suppliers. A striking feature of the German safeguards is that they cover the phases before, during and after a deployment. Another striking feature is that the safeguards mostly pertain to the integrity and reliability of the data collected. There is less emphasis on traceability of data.

4.10.1 Prior to a deployment

Both the statutory regulation and the SLB guideline express that technical tools may not record or modify a computer system more than is necessary. Data must be protected against modifications, deletion and unauthorised access by third parties. The SLB guideline further mentions that any modifications need to be traceable and that the transfer of communications must take place between the extracting software on the suspect's computer system and the registration and control unit of the executing authority.

In addition to the requirements imposed on technical tools, Germany also has a test procedure for approving software. It did not become clear who carries out these tests and who checks to see whether such tools meet the SLB guideline. Germany does not appear to have an authority similar to the Examination Service. Germany does have the ZITiS organisation. This organisation plays a role in research into and the development of technical tools by means of market research, for example, and by verifying whether such technical tools comply with German legislation.

4.10.2 During and after a deployment

The German Code of Criminal Procedure and the SLB guideline regulate that investigative authorities must log information (logging and documentation), if a technical tool is used for the collection of data. This must include, for example, information based on which the collected data can be determined. Logging and documentation must ensure the integrity of the data collected, i.e. that the data actually originate from the suspect's computer system, that they are complete and that they have not been manipulated. The SLB guideline also has two other safeguards

regarding data integrity during the deployment of the powers. First, only employees executing the power are given access to the data collected. This must be documented. Second, employees only receive those access rights that are necessary for the performance of their role. The software used must be archived for the traceability of the data.

Germany has a notification obligation that applies after the deployment of source interception or an online search. This means that persons in respect of whom the hacking power has been deployed will, in principle, be notified. If a case comes up for hearing, the quality of the data collected could be questioned based on the information they find in the file. The question will be to what extent that information provides sufficient leads to assess the data quality.

5 France

This chapter has been checked for factual inaccuracies by two lawyers from France. These individuals did not feel it necessary to be named.

5.1 Legal concept of computer data recording

On 14 March 2011, the French police were legally granted power to record computer data (*captation de données informatiques*).[112] This power made it possible for the police to remotely infiltrate computer systems[113] unnoticed. In the context of tackling organised crime and terrorism, the scope of the power was extended several times, namely in November 2014, August 2015 and June 2016 (Ministère de la Justice, 2019, p. 1).[114] The law was last amended on 23 March 2019. At that time, a common framework for three special investigative powers was created: the use of the IMSI catcher, interception of images and sound and the recording/capturing of computer data.[115] Under this law, computer data capture is regulated by three articles in the Code of Criminal Procedure (*Code de procédure pénale* or CCP) Article 706-95-11 CCP, Article 706-102-5 CCP and Article 15-1-6 CCP.

Computer data recording is defined in Article 706-102-1 CCP as follows: 'use of a technical device to access, record, store and transmit computer data, without the consent of the parties involved, as they are stored in a computer system, as they are displayed on a screen in front of the user of a computer system, as they are entered there by entering characters or as they are received and transmitted by audio-visual peripherals'.[116]

The power allows the police to record both stored and streaming data, meaning that stored data such as photos, videos and chats may be accessed. In addition, the power may also be used to intercept 'live' audio and video (Ministry of Justice, 2019, pp. 1-2). It is unclear whether it is also possible to turn on the microphone and camera for surveillance purposes. Interviews reveal that there is discussion about the scope of the power. There is a specific surveillance power that allows for covertly placing a microphone or camera;[117] however, nowhere in the Act is it explicitly stated whether this is also possible with the power that allows the recording of computer data. One of the interviewees from the French Ministry of Justice confirms that it is currently not possible to activate the microphone and camera from a distance in the scope of judicial proceedings (personal communication, 13 July 2023).

---

112 This power was introduced in the 'LOPPSI Act' of 14 March 2011 (Act No. 2011-267), which freely translated stands for the Act on Guidance and Programming for Internal Security (*Loi d'orientation et de programmation pour la sécurité intérieure*).

113 In France, reference is made to an automated data processing system (*Système de traitement automatisé de données* or STAD). This term has no legal definition, but case law shows that it is a broad concept. It can cover very different systems, such as data management infrastructures, bank cards, corporate computer systems and websites (Mattatia, 2015, p. 838).

114 The law of 13th november 2014 added the possibility to access data as received and emitted by audiovisual devices. The law of 17th august 2015 extended the scope of application to offences relative to economical delinquency, trafficking in cultural goods and illegal gambling activities. The law of 3rd june 2016 allowed prosecutors to use this technique, with the authorization of the 'liberty and custody judge'.

115 Act No. 2019-222, 23 March 2019, Programming 2018-2022 and reforming the justice system (*LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*).

116 See also Ministère de la Justice (2019).

117 Article 706-96 CCP.

5.2 Competent authorities

Like Belgium, France has two types of preliminary investigation: a criminal investigation and a preliminary judicial investigation (*information judiciaire*). In all types of investigation, the police may use the power to record computer data. The procedure to deploy the power differs for each type of investigation.

The criminal investigation is divided into two phases: *enquête flagrance* (flagrant investigation) and the *enquête preliminaire* (the preliminary investigation, not to be confused with the preliminary judicial investigation).[118] The *enquête flagrance* starts following red-handed cases or crimes that have just taken place (Verrest, 2018, p. 181). After eight, an *enquête preliminaire* or preliminary judicial investigation can be initiated.[119] Although the police are given a great deal of freedom to act independently during the *enquête preliminaire,*[120] the power may only be used after authorisation from the judge charged with matters of liberty and detention (*juge des libertés et de la detention*) at the request of the public prosecutor.[121]

In the following cases, the public prosecutor may decide to order a preliminary judicial investigation:
1 a preliminary judicial investigation is mandatory in case of a serious offence;[122]
2 initiating a preliminary judicial investigation is necessary to remand the accused in custody;[123]
3 initiating a preliminary judicial investigation is necessary because it requires certain investigative powers reserved for the investigating judge.

The investigating judge is charged with the investigation when the public prosecutor orders the preliminary judicial investigation. The offences to be investigated by the investigating judge are framed by the public prosecutor's demand. Only with a new demand from the public prosecutor may additional facts be investigated (Verrest, 2018, p. 184). After consulting the public prosecutor, the investigating judge may decide to use computer data recording for the investigation.[124]

Article D15-1-6 CCP lists agencies that may use the power. In summary, these include various components of the police, the intelligence service and the state police (*Gendarmerie Nationale*).[125] The actual technical implementation of the power lies with the national technical service for judicial records *Service technique national de captation judiciaire* (STNCJ). This service is officially part of the Ministry of Internal Affairs and is responsible for the centralisation and implementation of technical tools for recording computer data. The STNCJ also coordinates or – if necessary – carries out the operations to install the technical tools (Ministère de la Justice, 2019, p. 6). This organisation is discussed in more detail in 1.1.7.

---

118 Under French law there are three types of investigations frameworks: the 'enquête de flagrance', the 'enquête préliminaire', and the 'information judiciaire' (preliminary judicial investigation). For the overview the enquête de flagrance and the enquête préliminaire are combined under the umbrella term 'criminal investigation'.
119 For crimes carrying a prison sentence of five years or more the public prosecutor may decide to extent the sentence for a maximum period of eight days if this is needed to establish the truth.
120 Verrest (2018, p. 182) notes that initiating an *enquête preliminaire* is not subject to formal requirements and is often not reported to the public prosecutor. It is only after six months that the police has to inform the public prosecutor of the progress of the investigation.
121 Article 706-95-12 CCP.
122 Article 79 CCP.
123 Article 143-1 CCP.
124 Article 706-95-12 CCP.
125 The Gendarmerie Nationale is comparable to the Royal Netherlands Military Constabulary (KMar).

5.3 Against whom?

The French Act only mentions the type of serious offences for which the power may be used (see 1.1.4 for an overview of these offences). This means that computer data may in any case be recorded from the computer systems and systems of a person suspected of one of these offences. It is unclear to what extent – as in some other countries – the power may also be used for computer systems and systems of persons with whom the suspect communicates. Under Article 706-102-5 CCP, the power may explicitly not be used in a number of locations belonging to holders of confidential information, including the vehicle, office or home of senators, lawyers, judges and journalists.[126]

5.4 Cases

Under Article 706-102-1 CCP, the police may only record computer data in the case of offences of a terrorist nature,[127] organised crime[128] and serious economic crime.[129] With regard to organised crime, this concerns some 20 criminal offences (and preparations to commit them), described in Article 706-73 CCP, such as murder connected to organised crime, money laundering and drug trafficking connected to organised crime.[130] With regard to serious economic crime, it involves twelve criminal offences listed in Article 706-73-1, which include engaging in organised illegal employment, money laundering and illegal operation of casinos.

5.5 Term of authorisation

The time period within which the police may use the power depends on the type of investigation. In the context of the criminal investigation the power may be used for a maximum of one month, which period of use may be extended once by one month. In the context of the preliminary judicial investigation, a maximum period of four months applies. The use may be extended, under the same conditions, by up to four months each time, with the total period of use not exceeding two years.

5.6 Formalities

As mentioned before, the power to record computer data may be used during the criminal investigation and the preliminary judicial investigation. During the criminal investigation, an authorisation from the judge charged with matters of liberty and detention is required. During the preliminary judicial investigation, the investigating judge – after consultation with the public prosecutor – issues an authorisation.
For all types of investigation, the power may only be used in the case of the offences listed in 1.1.4. Unlike many other countries, France does not recognise a proportionality requirement other than a necessity requirement (Ministère de la Justice, 2019, p. 5). The decision to use the power must be supported by a reference

[126] Articles 706-102-5 CCP in conjunction with 56-1, 56-2, 56-3, 56-5 and 100-7 CCP.
[127] These are crimes and offences that constitute terrorist acts referred to in Articles 421-1 to 421-6 of the French Criminal Code (*Code pénal*).
[128] Both under Article 706-73 CCP.
[129] Article 706-73-1 CCP.
[130] Verrest (2018, p. 188) notes that not all crimes listed in Article 706-73 CCP make reference to operating as an association or terrorism in the offence description. This includes money laundering. This means that the power may also be used to investigate these types of offence.

to 'factual and legal circumstances' demonstrating the need for the use (Article 706-95-13 CCP). Mere need for information in the investigation is not enough to justify use of the power (Ministère de la Justice, 2019, p. 5). Under Article 706-102-3 CCP, the authorisation must include the following elements:

- the nature of the offence for which the power is being used;
- the exact location or detailed description of the computer systems and systems;
- the period of use.

If there is an immediate risk of loss of evidence or serious harm to persons or property, the investigating judge may issue an authorisation in a preliminary judicial investigation, under Article 706-95-15 CCP, without first obtaining the opinion of the public prosecutor. The authorisation must contain the factual circumstances demonstrating the imminent risk. This accelerated procedure is not available for the criminal investigation.

5.6.1 Use of technical tools

Technical tools may be used to record computer data. To place the technical tool, access to the computer systems and systems may be obtained either physically or remotely.[131] The method of access determines the authorisation(s) required.

To physically place a technical tool, an official may be authorised to enter a vehicle, private place or dwelling without the knowledge of its occupant or user. Article 706-102-5 CCP distinguishes between entering these locations during and after 'statutory hours'. These hours refer to the times used for conducting searches of premisses. Under Article 59 CCP, these searches should take place between 6.00 and 21.00. For the physical placement of a technical tool, the following procedures can be distinguished:

- Criminal investigation: the judge charged with matters of liberty and detention issues the authorisation at the request of the public prosecutor. If placement of the technical tool takes place outside statutory hours, a separate authorisation has to be issued. In that case, the judge charged with matters of liberty and detention will have to rule on both requests.
- Preliminary judicial investigation: in principle, the authorisation is issued by the investigating judge. If use takes place outside statutory hours, an authorisation must be obtained from the judge charged with matters of liberty and detention for this purpose.

If it is decided to remotely place the technical tool on the computer systems and systems, the 'normal' route is followed as described at the beginning of 1.1.6.

5.7 Use of technical tools to record computer data

The French Act prescribes no specific criteria that a technical tool must meet. Information about technical tools is state secret, as the devices can also be used by the French intelligence service (personal communication, 29 June 2022). In France, criminal procedure law in principle allows the use of resources that fall under state secrets.

[131] Article 706-102-5 CCP describes both routes.

The development of technical tools for recording computer data has been made the responsibility of the STNCJ mentioned above.[132] The technical tools that fall under the power therefore depend on the STNCJ. The activities of the STNCJ are qualified as state secrets,[133] so it is not clear what criteria they apply for developing or procuring technical tools.

5.8 Safeguards

With regard to the recording of computer data, there are a number of general conditions that help ensure the quality of the data.[134] Article 706-95-18 CCP regulates that a report describing the operations and installation of the technical tool must be prepared by the public prosecutor or the investigating judge (or a police officer appointed by them). It must include the date, time of the start and end of the activities. Only the data necessary for establishing the truth may be copied. Data relating to the suspect's private life must be deleted. If the data are in another language, they must be transcribed in French. The data must be kept 'sealed', in the case of the present power by the STNCJ. When the statutory limitation period expires, they are destroyed by order of the public prosecutor, and a record is made of the destruction.[135]

5.8.1 Judicial review

The execution of the power takes place under the supervision of the judge granting permission.[136] In the case of the criminal investigation, this is the judge charged with matters of liberty and detention and, in the case of the preliminary judicial investigation, the investigating judge who must act within the demand formulated by the public prosecutor. The judge can terminate the use of the power at any time. To do so, the public prosecutor must inform the judge in good time about the activities conducted under the power. If the judge determines that the power has not been exercised within the specified framework, the collected data must be deleted. If the power has been used for purposes other than those specified in the authorisation, the collected data may be declared invalid by the trial judge.

5.8.2 National Technical Service for Judicial Records (STNCJ)

In 2018, the National Technical Service for Judicial Records was established.[137] This organisation is responsible for the design, centralisation and implementation of the technical tools used for recording computer data.[138] The service also coordinates or – where necessary – implements the use of the technical tools.[139] As already noted, the service's activities are state secret.[140] As a result, it is unclear what criteria it uses when developing or procuring technical tools. Since STNCJ is responsible for sealing

[132] Decree of 9 May 2018 establishing the service with national competence called the 'national technical service for judicial records'. JORF no. 0107, 10 May 2018 ('Decree 9 May 2018').
[133] Article 3, Decree of 9 May 2018 establishing the service with national competence called the 'national technical service for judicial records'.
[134] These safeguards also apply to the use of other special investigative powers.
[135] Article 706-95-19 CCP.
[136] Article 706-95-14 CCP
[137] Decree 9 May 2018.
[138] Article 2, Decree 9 May 2018.
[139] Article 2, Decree 9 May 2018.
[140] Article 3, Decree 9 May 2018.

and preserving the data, it has a role in protecting the integrity of the data collected.[141]

In 2018, based on Article 5 of the Decree of 9 May 2018, a Strategic Committee was established, consisting of the Minister of the Interior, the Minister of Justice and representatives of the services using the power. The Committee submits proposals for 'the strategic commitments' and resources necessary for the proper functioning of the service. It also oversees the accounts and adopts the service's internal regulations,[142] The Committee also writes reports on the service operations and some of these are shared with parliament (Personal communication, 12 september 2022). In addition to the Strategic Committee, two persons are appointed by the Minister of the Interior and the Minister of Justice to oversee the operations of the service.[143] These persons will have full access to all technical tools and operations of the service. They may also request the service to provide any additional information they deem necessary to perform their duties. Every year, they prepare an annual report and this is provided to the Minister of the Interior and the Minister of Justice. This report is not public and qualifies as a state secret.

5.8.3 Notification obligation and right of access to documents

The Act contains no notification obligation, and a defendant will therefore only be notified when a case goes to trial – if the use of the power has produced evidence which has been included in the case file. 'In the preliminary judicial investigation, the defence has access to the procedural documents (Article 116 CCP) and can contribute to the establishment of the truth by requesting investigative actions (Article 82-1 CCP)' (Verrest, 2018, p. 180).

5.9 Case law

Operating as a Joint Investigatory Team (JIT), French and Dutch authorities managed to hack into the communication service EncroChat. For a short period, the authorities could read all messages exchanged by criminals in real time. As the servers were located in France, it was the French police who carried out the hack (Goodwin, 2022). The hack produced over 120 million messages from 60,000 users. The messages were used as evidence in many countries, provided through a request for legal assistance. In France, too, EncroChat data has been used as evidence. This has led to two rulings relevant to the present investigation, and more rulings may follow.

The first ruling is from April 2022, in which the Constitutional Council (*le Conseil Constitutionne*) decided that resources that are classified as state secrets can be used in criminal proceedings.[144] As a result, there is no need to share information on how hacked data was obtained. However, a Court of Cassation (*Cour de cassation*) ruling appeared in October 2022, in which the court concluded that it is necessary for additional information to be shared when making use of the power.[145] Two of the three defences concerned the legality of the power and were rejected by the Court of Cassation, the third defence was partially upheld. Under Article 230-3 CCP, in case of decryption of data or communication, technical details of data recording must be

[141] Article 706-95-18 CCP.
[142] Article 6, Decree 9 May 2018.
[143] Article 7, Decree 9 May 2018.
[144] Constitutional Council, no. 2022-987 QPC, 8 April 2022.
[145] Court of Cassation, Criminal Division, 11 October 2022, appeal no 21-85.148.

provided. The head of the operating technical organisation must also provide a signed 'certificate of truthfulness'. This certificate confirms the accuracy and authenticity data used as evidence (Goodwin, 2022). The Court of Cassation held that these two criteria had not been sufficiently tested and therefore referred the case back to the lower court. In a later ruling the Court of Cassation concludes that while the certificate is a procedural obligation, but ruled that this is only necessary when the data collected is encrypted. In the Encrochat case the data collected was already decrypted before it was recorded by the police, and as such the certificate was not needed (Niculai, 2023).

5.10 In conclusion

Since 2011, it has been possible for the French police to covertly record computer data remotely on computer systems and systems. The covert recording of computer data basically makes it possible to carry out any investigative action (depending on the authorisation issued by the investigating judge). An exception to this rule is the performance of surveillance using the microphone or camera present at the computer systems and systems; it is as of yet unclear whether this falls within the scope of the Act.

There are some general safeguards that also apply to other special investigative powers, including the sealed storage of data obtained and the method of reporting on actions carried out. The main difference compared to the Netherlands is that the judge not only issues the authorisation, but also su6pervises the execution in the interim and that the judge may abort the use at any time if there is any reason to do so.

Another important safeguard for the power is the presence of the STNCJ service. This service, like Digit in the Netherlands, implements the power with the help of technical tools. Unlike in the Netherlands, France has no examination service for the technical tools. The STNCJ also fulfils this task to some extent, though it is not known how the STNCJ implements the power. Because the service also develops technical tools for the intelligence service, its doings are less transparent than those of Digit. And the same applies to the supervision of the STNCJ. Publications by regulators on the service's doings are not made available to the public (state secret). This contrasts with the work of the Inspectorate in the Netherlands, which does publish a public report. It is striking that the STNCJ is both 'supervisor' and 'implementer'. This may raise the question to what extent the STNCJ can independently perform both roles. Nevertheless, the service is highly regarded in France and the fact that it carries out the operational task is, as such, seen as a safeguard. Among other things, the STNCJ is responsible for storing and sealing the data.

6 Sweden

Special thanks to Johanna Rådberg (police, Sweden), Chatrine Rudström (Public Prosecution Service, Sweden), Pär Runemar (police, Sweden) and Staffan Uhlmann (Ministry of Justice, Sweden) for critically reading this chapter for factual inaccuracies.

6.1 Secret data reading

The Secret Data Reading Act (*Lag om hemlig dataavläsning*), hereinafter abbreviated to SDRA, came into effect in Sweden on 1 April 2020.[146] The Act makes it possible for the Swedish police, via covert and remote surveillance, to read or record information in a computer system[147,148] If necessary, a computer system may be penetrated for this purpose.[149] The introduction of the Act was deemed necessary by the legislature for two reasons: 1) the need to covertly access information that technological and societal developments have rendered inaccessible using existing coercive measures, and 2) a need to covertly collect data on the operation and use of computer systems that cannot be obtained via existing coercive measures.[150]

Authorisation may be granted to record the following types of data:[151]

1 Communication interception data: data on the content of messages sent to or from a telephone number or IP (or other) address.
2 Communication monitoring data: non-content meta (and other) data about communications that take place to or from a telephone number or address.
3 Location data: information about the location of the computer system.
4 Camera surveillance data: information obtained through the camera of the computer system.
5 Physical interception data: data collected by means of the microphone of the computer system in physical spaces.
6 Data that is stored in the computer system.
7 Data that shows how the computer system is used.

Contrary to what its name might suggest, the Act allows not only stored data, but also streaming data to be collected. The camera and microphone in the computer system may also be turned on for the purpose of obtaining data.

6.2 Competent authorities

In Sweden, both the police and the public prosecutor can initiate a preliminary investigation (criminal investigation). The person in charge of the preliminary investigation is referred to as the 'investigation leader' *(undersökningsledaren*) (Wong, 2012, p. 3-4). The public prosecutor assumes responsibility for conducting an

146 Lag (2020:62) om hemlig dataavläsning Svensk författningssamling.
147 In Sweden, reference is made to a 'readable computer system' *(avläsningsbart informationssystem*), which is defined as: 'an electronic communication device or user account for, or an equivalently demarcated part of, a communication service, storage service or similar service' (Section 1 SDRA).
148 Section 1 of the SDRA.
149 Section 22 of the SDRA.
150 Proposed Swedish Secret Data Reading Act, p. 68-73.
151 Section 2 of the SDRA.

investigation as soon as someone is reasonably suspected of the offence.[152] The investigation leader determines which investigative powers are to be used during an investigation and how and when the investigation is completed. The actual investigative measures – such as interrogation and the execution of investigative powers – are in practice carried out by the police. Some of these measures – such as surveillance powers – require a court order (Wong, 2012: p. 4).

As the power to conduct the covert surveillance of data can, in principle, only be exercised when someone is reasonably suspected of the offence, in practice it is the public prosecutor who will order the covert surveillance of data to be carried out in a criminal investigation.[153] Section 15 of the SDRA provides that a court authorisation is required to exercise the power. In addition to the court, a 'public representative' is also involved who represents the suspect's interest in relation to the assessment of the application.[154] In urgent cases, the prosecutor themselves may grant authorisation pending the court's decision.[155] The public prosecutor is then required to inform the court 'without delay'.

The Act does not prescribe which part of the police authorities is charged with the actual exercise of the power. An interview with the Swedish police reveals that, in practice, a police team with technical expertise is charged with this responsibility.[156]

6.3 Against whom?

Analogous to the existing interception powers in Sweden, the power can, in principle, only be exercised against someone who is strongly suspected of one or more offences.[157] In accordance with Section 4 of the SDRA, the power may furthermore only be exercised in respect of the computer system being used by the suspect. Section 4 of the SDRA does, however, allow for the power to be exercised in the context of communications interception in respect of a computer system with which it is strongly suspected the suspect will establish contact (e.g. a loved one's phone). Section 5 of the SDRA also provides a second exception, in situations where a computer system is found that was used during the crime or is connected with the crime scene. In that case, the power may be exercised to retrieve communication monitoring data and location data in order to ascertain the possible identity of someone suspected of the offence.

6.4 Cases

In the preliminary investigation, the power may be exercised for offenses with a minimal penalty of two years' imprisonment.[158] In addition, Section 4 of the SDRA lists a number of specific offences for which the power can be exercised. They include:

[152] Chapter 23, Article 3 of the Swedish Code of Judicial Procedure. This article also provides for the public prosecutor to take over the conduct of the investigation in other cases if 'special reasons' so require.
[153] Section 5 SDRA provides an exception in which the power can be used to discover the identity of a suspect. In this case, the police may still be in charge of the investigation. However, the technical aid must always be used by the public prosecutor in accordance with Section 14.
[154] Section 16 of the SDRA. Also see Subsection 1.1.5.
[155] Section 17 of the SDRA.
[156] Personal communication, 6 july 2022.
[157] Proposed Swedish Secret Data Reading Act, p. 109. Chapter 27, Article 20 of the Swedish Code of Judicial Procedure.
[158] Section 4 of the SDRA.

sabotage, arson, threats to the legal order, industrial and other espionage committed by foreign powers and terrorism.[159] This also applies to attempt, preparation or conspiracy to commit the offences referred to above.[160]

Outside the framework of the preliminary investigation, the power may be exercised for a number of other specific purposes. First of all, the power may be exercised to prevent 'particularly serious' offences *(särskilt allvarliga brott*).[161] These include the aforementioned offences, plus murder, manslaughter, aggravated assault, abduction or unlawful deprivation of liberty.[162] The power may also be exercised where there is a 'material' risk that an individual or group will commit one of these offences. In addition, the police may covertly collect data for the purpose of implementing the Aliens Act, for example in the case of a deportation decision.[163] As this concerns specific exceptions and/or preventive measures, the remainder of the chapter focuses on the use of secret data reading in the preliminary investigation.

Section 11 of the SDRA also provides for various situations in which the power may not be exercised. Secret data reading is prohibited where its exercise in respect of a computer system restricts the freedom of the press and if a holder of confidential information, such as a lawyer, doctor or priest, uses the computer system.

6.5 Term authorisation

The power may not be exercised for longer than is necessary. The maximum period is one month, and may be extended by successive one month periods. No time limit applies to historically stored data, such as text messages on a telephone. This therefore means that historical text messages or emails can also be read and stored outside the time limit under the authorisation.[164]

6.6 Formalities

The public prosecutor needs to apply for a court authorisation in order to exercise the power in a preliminary investigation.[165] A court order can only be issued for offences listed in Subsection 6.4 and, under Section 3 of the SDRA, may only be granted if the reasons for the exercise of the power outweigh the intrusion or infringement brought about by the power (principle of proportionality). The interviews reveal that the judge's assessment focuses on the provisions in the SDRA and related provisions. It is unclear to what extent the court looks at the technique of the tools and at the associated guarantees. A decision by the Swedish Commission on Security and Integrity Protection ('Säkerhets- och integritetsskyddsnämnden'), hereafter SIN, shows that technical experts from the police are sometimes heard by the judge.[166] Based on this decision and information from interviews, it appears that the focus is on the technical aspects that influence the proportionality of the deployment, for example the investigative actions that can be performed with the tool.

159 Chapter 27, Article 18, Paragraphs 2 to 7 of the Swedish Code of Judicial Procedure.
160 Chapter 27, Article 18, Paragraph 8 of the Swedish Code of Judicial Procedure.
161 Section 7 of the SDRA.
162 Section 1, Act (2007:979) on measures to prevent certain particularly serious offences (*Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott*).
163 Section 9 of the SDRA.
164 SIN Statement, 2021, p.6.
165 Section 15 of the SDRA.
166 SIN Statement, no. 92-2020.

Section 18 of the SDRA prescribes that the authorisation must include a number of elements. Firstly, the start date and time limit of the authorisation must be stated. Secondly, the specific computer system to which the order relates must be laid down (see paragraph 6.8.2). Thirdly, it must be specified which types of data are intercepted or recorded: for example, communication monitoring data and camera surveillance data (see paragraph 1.1.1). Fourthly, a record must be kept of the specific measures taken to minimise the intrusion or infringement in respect of the subject. For example, that the camera or microphone in a computer system may only be activated at a certain time or location. Finally, in the case of interception, the name of the individual who is suspected of the offence must be specifically registered.

6.6.1 Public representative

On receiving an application from the public prosecutor for authorisation to exercise the power, the court must appoint a public representative at the earliest opportunity.[167] The public representative must be a Swedish citizen and be or have been a lawyer or ordinary judge.[168] The role of public representatives is to protect the suspect's privacy interests in relation to the assessment of the application. The representative has the right to participate in what emerges in the case and to advise on the application. The representative's advice is not binding on the court's assessment. However, the representative may appeal against the court's decision if they disagree with that decision.[169]

6.7 Use of tools for the covert surveillance of data

Once the authorisation has been issued, the police may use any tools (usually software) that is required to intercept and store data.[170] The only restriction specified in the law is that the tools must be adapted to the authorisation contained in the order.[171] Section 23 of the SDRA provides that the tools must be adapted in such a way that it is not possible to intercept or store information other than as specified in the order. The tools need not have been developed specifically with a single purpose in mind. As long as the police can demonstrate that the software was used *only* to intercept and record the data in accordance with the order then that is sufficient to meet the condition set out in Section 23 of the SDRA. If it is established that data falling outside the scope of the order has nonetheless been recorded, that data should be immediately deleted and a notification made to the Swedish Commission on Security and Integrity Protection *(Säkerhets- och integritetsskyddsnämnden*, hereinafter: 'SIN'). The Commission's role is discussed in greater detail in paragraph 1.1.7.

6.8 Safeguards

The Act makes little mention of formal safeguards regarding the quality of data obtained through covert surveillance of data. Sections 25 and 26 of the SDRA list a number of due care requirements, however. A role is also assigned to SIN, the special supervisory commission, which oversees the manner in which the secret data reading

[167] Section 16 of the SDRA.
[168] Chapter 27, Article 27 of the Swedish Code of Judicial Procedure.
[169] Chapter 27, Article 26 of the Swedish Code of Judicial Procedure.
[170] Section 22 of the SDRA.
[171] Section 23 of the SDRA.

is carried out, amongst other things. In addition, the police have various internal guidelines on how the power is to be exercised. These guidelines are not publicly accessible. Finally, there is a notification requirement and the suspect is given a copy of the data obtained using the power. The above points are discussed in greater detail in the following paragraphs.

6.8.1 Due care requirements

Sections 25 and 26 of the SDRA list a number of due care requirements that may have an indirect impact on the quality of data in the computer system. The primary focus of the requirements is that the actions performed should not cause any nuisance or damage to or in the suspect's computer system beyond what is strictly necessary for the exercise of the power. The tools should be removed after use and the security of the computer system should be at least at the same level as before the tools were deployed. In addition, Section 26 includes the requirement that the individuals exercising the power should have sufficient knowledge and qualifications to exercise the power.

6.8.2 Commission on Security and Integrity Protection (SIN)

SIN supervises the use by the Swedish Police and the Swedish Secret Service of special investigative means and procedures.[172] As a result, SIN also supervises the use of covert surveillance of data. SIN's aim is to 1) check whether special investigative powers are exercised in accordance with laws and regulations and 2) whether personal data are processed in accordance with laws and regulations.[173] The Commission has a maximum of ten members. The chair and vice-chair have a legal background (they are judges, for example), while the other members are appointed from the persons proposed by the party groups in the Swedish Parliament (12 September 2022). The Commission has limited technical knowledge, and can appoint a competent or expert person for assistance, if necessary.[174]

The court is obliged to notify SIN upon the issue of a court authorisation for covert surveillance of data.[175] In theory, SIN can make any matter of which it is notified subject to its supervision. In response to written questions, SIN states that the selection is made on a random basis. In addition, the selection may be made on the basis of irregularities in the notification, for example because the offence does not qualify for the use of the power.[176] SIN is also obliged, at the request of an individual, such as a suspect against whom the power has been exercised, to check whether that individual has been subject to measures under the power and, if so, whether this was carried out in accordance with the law.[177] SIN must notify the individual that the check has been carried out. If, in SIN's view, the individual's request is 'unreasonable' or 'unfounded', no check need be carried out.

If SIN identifies irregularities, it issues a ruling. While SIN's rulings are not binding, in a written response SIN states that, in principle, the organisations follow SIN's rulings

[172] Supervision of Certain Law Enforcement Activities Act (2007:980) *Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet*.
[173] Section 3 of the Supervision of Certain Law Enforcement Activities Act (2007:980).
[174] Article 18 of the Ordinance with instruction for The Commission on Security and Integrity Protection (2007:1141). *Förordning (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden*.
[175] Section 21 of the SDRA.
[176] Personal communication, 26 august 2022.
[177] Section 3 of the Supervision of Certain Law Enforcement Activities Act (2007:980).

and adjust their internal guidelines accordingly.[178] If irregularities are so serious that they constitute a punishable offence (e.g. in case of abuse of office), the matter will be reported to the Public Prosecutor's Office, which may decide to prosecute.[179]

Other than the legality assessment, there are no additional criteria contained in laws and regulations at which the supervision is aimed. SIN furthermore does not use an examination protocol. In its written response, SIN states that supervision of this power is still evolving. Nonetheless, two rulings issued in 2021 shed a little more light on the criteria that are under consideration:[180]

- Compliance with fundamental legal conditions;
- The period during which secret data reading is carried out;
- The proportionality of the use of the power in relation to the type of data that is read during the use of the power;
- The conditions in the court order aimed at safeguarding the suspect's personal integrity;
- The exercise of the power in relation to other conditions in the court order;
- Requirements of due care and accuracy when exercising the power.

Although the conditions described are mainly legal in nature or process-related, the above criteria could also concern the tools used, e.g. the functionalities of the tools. The public prosecutor is obliged to make a report to SIN in the event any tools inadvertently yields more information than is covered by the scope of the order. SIN can also determine this itself during its supervision activities. This can then result in certain tools no longer being usable or having to be modified.[181]

6.8.3 Internal guidelines for covert surveillance of data

Although the law includes few formal safeguards regarding the quality of the data obtained from data reading, the police do have various internal guidelines on the exercise of the power and the use of tools, and these guidelines continue to be developed.[182,183] SIN has indicated that at the time of their ruling, uniform internal guidelines were still absent at the Public Prosecutor's Office.[184]

As the police's internal guidelines are confidential and not publicly available, we have been unable to ascertain which internal criteria the police apply regarding the quality of data obtained through covert surveillance of data. Interviews reveal that the police use standardised or certified software. It is explained that, at the hearing, this software can be used as one of the arguments demonstrating that the integrity of the data processed in this software is guaranteed. For software that is not specifically used for data reading, the Swedish National Forensic Centre can evaluate the tools. This includes, for example, tools that permits the initial or further analysis of intercepted data. This tool is not used to hack into a computer system, but can therefore be used at a later stage of the secret data reading – after the data has been obtained. In

[178] Personal communication, 29 September 2022.
[179] Personal communication, 26 august 2022; Cameron, I. (2021). Sweden in Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis. P. 1365 Berlin: Duncker & Humblot.
[180] Number 96-2022 Statement SIN, Number 92-2020 Statement SIN.
[181] Personal communication, 29 September 2022.
[182] Number 92-2020 Statement SIN.
[183] See also the SIN ruling following a case in which the power was exercised in respect of the wrong phone. This led to the police's internal guidelines being amended to include more checks in the process to prevent the tools from being used in respect of the wrong automated computer system. Number 96-2022 Statement SIN.
[184] Number 92-2020 Statement SIN, p. 15.

addition, tools that is viewed as the standard within other police authorities[185] or has been certified by them (e.g. by the Dutch Police technical appraisal office) is also used.

6.8.4 Notification obligation and right of access

Section 28 of the SDRA in conjunction with Chapter 27, Article 31 of the Swedish Code of Judicial Procedure provide for a notification obligation to data subjects. In accordance with Chapter 27, Article 31 of the Code of Judicial Procedure, an individual must, in principle, be notified as soon as possible, and no later than one month after the preliminary investigation is completed. The notification should state which special investigative means and procedures were used, and when they were used. The telephone numbers, IP addresses as well as other addresses and computer systems to which the measures applied must also be stated. In the case of physical interception of images or sound, information on where the interception took place must also be included.[186] Chapter 27, Article 33 of the Swedish Code of Criminal Procedure provides that a notification is not required if the preliminary investigation concerns the offences referred to in Paragraphs 1 to 7, which mainly are crimes that threaten public or national security. This includes many of the crimes for which secret data reading can be used.

If the public prosecutor decides to launch a prosecution and the case comes to trial, often this will also be the moment when a suspect is notified. The suspect is given access to the evidence used in court. The suspect can, substantiated, ask for additional information that has been collected. In the case of covert surveillance of data, this means that they receive a copy of all the data that has been collected. The interviews with Swedish respondents reveal that experts can be called as witnesses if there are questions about the quality of data. The interviews show that the public prosecutor may call the police officer concerned as a witness to explain what actions were taken and why the quality of the data is assured.[187] However, no information is shared about the tools used or the modus operandi of the police.[188] Sweden furthermore has a flexible regime as regards admissible and free evaluation of evidence, as provided in Chapter 35, Article 1 of the Code of Judicial Procedure. In principle, all evidence is admissible, regardless of how it was obtained. It is up to the court to weigh how relevant the evidence is (Klamberg, 2020). The methods for obtaining the evidence may affect the evaluation of the evidence, and in flagrant cases the evidence may be disregarded by the court.

6.9 Case law

A letter submitted to parliament reveals that the power has been used in 205 criminal investigations since the Act entered into effect.[189] As far as we are aware, however, there is no existing case law concerning cases in which the power was used. Nevertheless, there are a few judgments in cases involving evidence obtained from communication using the EncroChat system. In these cases, the quality of the data

[185] An example of this type of software is Cellebrite, which many police authorities use to extract, read and analyse data from mobile devices.
[186] Section 29 of the SDRA in conjunction with Chapter 27, Article 32 of the Swedish Code of Judicial Procedure.
[187] Personal communication, December 13, 2022.
[188] Personal communication, December 13, 2022.
[189] Government letter 2022/23.30, Accountability regarding the use of covert coercive measures. in 2021 This involved 145 criminal investigations in 2021 and 60 criminal investigations in 2020 (from April).

obtained was also called into question. There is also a ruling by SIN following the improper use of the power.

On 26 February and 22 April 2021, the Svea court of appeal gave judgments in cases in which communication using the EncroChat system[190] was put forward as evidence.[191] The defence submitted similar arguments in both cases. The first objection related to the legality of the evidence, and was rejected by the court. As this does not concern the quality of the data obtained, this will not be discussed any further. Various issues were raised regarding the quality of the data. These include missing messages, some messages having the same sent time meaning there is a possibility they might be read in the wrong order, and the data having been edited (copied by the police) several times. The court acknowledged that the data is incomplete and that it is important to assess the messages carefully in their context. The court added that the data, in conjunction with other investigation data, show that 'the messages correspond well to reality in terms of time and content'.[192] In both cases, the court rejected the defence's objections.

These two judgments are joined by a SIN ruling of 16 November 2021 following the improper use of covert data collection in a criminal investigation. In the investigation in question, the power had been mistakenly used in respect of a mobile phone not covered by the order. Upon discovery of the mistake, use of the power was halted and the data was immediately deleted. SIN concluded in its ruling that the case showed that the requirements of due care and accuracy had not been met and that appropriate measures should have been taken earlier.[193] The police changed their procedures following the ruling. They now conduct multiple checks to ensure that the power is used in respect of the right system.[194]

6.10 In conclusion

The Secret Data Reading Act makes it possible for the Swedish police, via covert and remote means, to penetrate a computer system and to read the data in the computer system. Based on the Act, the following types of data can be reviewed: communication interception data, communication monitoring data, location data, camera surveillance data, physical interception data, data in the computer system and data that shows how the computer system is used. The Act does not stipulate any specific requirements in respect of the tools that can be used (commercial or self-developed).

The Act makes little mention of formal legal requirements regarding the quality of the data obtained through use of the power. However, the police authorities have internal policy rules detailing further processes and requirements in relation to the use of tools. As these guidelines are unfortunately not publicly accessible, it is unclear how far their scope extends. A notable fact, when compared with the Netherlands, is that the

[190] EncroChat was an encrypted communications service used by criminals to communicate anonymously. The servers of this communications service were located in France and in 2019, intervention by French and Dutch law enforcement authorities meant that it was possible to read all the messages in unencrypted form for several months. In the wake of this, the data was also provided to various countries insofar as it related to suspects from the countries in question. See also: www.om.nl/actueel/nieuws/2022/10/12/om-verdachten-encrochat-behulpzaam-aan-alle-strafbare-feiten-klanten.

[191] Judgment given by Eskilstuna District Court on 26 February 2021 in case no. B 210-21 & Judgment given by Stockholm District Court on 22 April 2021 in case no. B 5546-20.

[192] Judgment given by Stockholm District Court on 22 April 2021 in case no. B 5546-20, p. 9.

[193] Number 96-2022 Statement SIN, p. 1.

[194] Number 96-2022 Statement SIN, p. 3.

principal checks with regard to the use of tools are carried out *ex post* by the supervisory commission SIN. SIN supervises the use of special investigative means and procedures, including covert surveillance of data. SIN's role in relation to the use of the tools for secret data reading is still evolving. For the time being, supervision is focused primarily on legal and process-related aspects of the power. However SIN can also subject specific tools to closer examination. Unlike the inspectorate in the Netherlands, SIN can both assess the actions of the police and the public prosecutor. It can also determine upon request by the subject or on its own behest whether or not the actions in individual cases are legitimate.

7 Switzerland

This chapter has been checked for factual inaccuracies by a lawyer from Switzerland. This person did not feel it necessary to be named.

7.1 Statutory regulation

Since 1 March 2018, the Swiss Code of Criminal Procedure (toevoegen hierna CCP) (*Schweizerisch Strafprozessordnung*) has included Article 269ter, which covers the hacking power. This article was announced in the explanatory notes (*Botschaft*) on the revision of the BÜPF, the Federal Act on the Surveillance of Post and Telecommunications (*Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs)*.[195] An important reason for this new legal provision was the encryption of communications (data), which meant that pre-existing powers for the police no longer provided useful information.[196] Paragraph 1 of Article 269ter CCP stipulates that the public prosecutor may order the installation of special software (*besonderen Informatikprogrammen*) in a computer system used for data processing (*Datenverarbeitungssystem*). The special software is referred to as Government Software, also known as GovWare (EJPD, 2019). Only communications and the telecommunications' metadata may be intercepted with the use of GovWare.
Prior to the introduction of the aforementioned power, there was a discussion on the question whether pre-existing articles of law already provided sufficient legal basis to install GovWare, for instance situations in which the Public Prosecution Service (*Staatsanwaltschaft*) is allowed to use technical monitoring equipment (*Überwachungsgeräte*).[197] While a majority of scholars considered that this did not fall under the scope of the article, some believed that this could be covered by the mentioned article, provided that Article 280 CCP would be broadly interpreted.[198] At the time of the introduction of the new legal provision, the Federal Supreme Court (*das Bundesgericht*) had not yet ruled on this matter,[199] nor has it at the time of writing of this report (see below).[200] Furthermore, it is known that judicial authorities had used GovWare prior to the introduction of the new CCP in 2011. That had been done on the basis of federal laws and laws in the Swiss cantons[201] (Basanisi, 2019, p. 2). Switzerland is made up of 26 different federal states (cantons). Switzerland also has a central state (ProDemos, no date).[202]

---

195 Since the introduction of the modernised Swiss Code of Criminal Procedure in 2011, the criminal procedural laws from the BÜPF have been transferred to the new Swiss Code of Criminal Procedure. For this reason, the revised BÜPF also introduced amendments to the Swiss Code of Criminal Procedure (Botschaft 27 February 2013, page 2690). One of these amendments is the introduction of Article 269ter CCP. Inclusion in the Swiss Code of Criminal Procedure further corresponds to a number of motions that had been submitted (Botschaft 27 February 2013, page 2777).
196 Botschaft 27 February 2013, page 2775.
197 Hansjakob (2011, page 5) argues why this article could not be used. He also argues that there is no statutory basis for the use of GovWare based on former Article 269 CCP (Hansjakob (2011, page 4).
198 Botschaft 27 February 2013, page 2772.
199 Botschaft 27 February 2013, page 2772.
200 There is also debate as to whether Art. 269 ter Sv and 280 Sv can be used together, for example for the deployment of a keylogger. Art. 269 would then be used to obtain encrypted communication. Once GovWare has been installed, keylogger functionalities could then be used (personal communication, April 16, 2023). The Federal Court of Justice ('Bundesgerichtshof') has given permission for the use of keylogger software based on art. 280 Sv, after the coercive remedies court of the canton of Zurich did not give permission for this. According to the Federal Court of Justice, no distinction needs to be made between hardware and software, as long as both function in exactly the same way.
201 Botschaft 27 February 2013, pages 2772-2773.
202 ProDemos template.

As previously described, Article 269ter CCP is directed at intercepting (encrypted) communications. This article does not allow online searches[203] or the use of cameras or microphones for purposes other than monitoring telecommunications. Observing a room with the use of GovWare is thus not allowed.[204,205] If data other than communication data are collected, these may not be used as evidence and must be destroyed.[206]

7.2 Competent authorities

As previously mentioned, Switzerland is made up of 26 cantons and one central state. Such a division is also reflected within the different institutions that operate within the criminal procedure sector. Principally, many criminal cases are dealt with at the level of the cantons. Still, some criminal cases are processed at the federal level. These criminal cases involve investigations into organised crime, offences against the State and economic offences, including money laundering. An important prerequisite is that the offences are committed abroad predominantly or that the offences cover multiple cantons and 'no clear area of focus of the criminal offences can be determined'. If the foregoing applies, cantons may request to have a federal court decide on the matter. In that case, the Federal Public Prosecution Service will initiate an investigation[207] (Godenzi & Caprara, 2018, page 284).

As previously mentioned, the use of GovWare is only permitted if ordered by a public prosecutor, at federal level or at the level of the cantons.[208] In addition to an order issued by the public prosecutor, a judge of the Coercive Measures Court[209] (*Zwangsmaßnahmengericht*) also needs to authorise the order.[210] This judge is comparable to the Examining Magistrate in the Netherlands. Amongst other things, this authorisation is to ensure that the parties concerned are protected against possible abuse of GovWare.[211] This court's supervision takes place *after* the Public Prosecution Service institutes the measure (*ex post)* (Godenzi & Caprara, 2018, page 299). Within 24 hours after having issued the order, the public prosecutor must submit the order to the Coercive Measures Court, including a substantiation for the deployment of the measure and the case documents relevant for the decision-making by the Coercive Measures Court.[212] Within five days of an order being issued, the Coercive Measures Court makes and explains its decision. The Court may subject the authorisation for deployment of the power to a time limit or request further information and a further investigation.[213] The Coercive Measures Court immediately notifies its decision to the public prosecutor and the post and telecommunications surveillance office within the meaning of Article 3 BÜPF.[214] The decision establishes the

[203] This would also follow logically from the fact that the person subject to a search must be informed accordingly. See Article 247 CCP. A suspect is not informed when GovWare is used. After all, the use of GovWare would then no longer serve a purpose (Botschaft 27 February 2013, page 2779).
[204] Botschaft 27 February 2013, page 2702; page 2776; page 2779.
[205] Betschamnn and Murer Mikolásek (2018) describe a discussion involving the possibility of combined use of Articles 269ter and 280 CCP to allow for a microphone or camera to be switched on. This is not possible according to both authors because this may also cover the recording of private communications unrelated to telecommunications traffic (Betschamnn & Murer Mikolásek, 2018, page 751).
[206] Article 269ter(3) CCP; Article 141(1) CCP; Article 277 CCP; Botschaft 27 February 2013, page. 2776.
[207] Article 16 CCP and Article 7 of the Swiss Judiciary Act (StBOG).
[208] Article 269ter(1) CCP.
[209] The Public Prosecution Service must generally seek authorisation from a court for the use of covert powers (Godenzi & Caprara, 2018, page 301).
[210] Article 272(1) CCP.
[211] Botschaft 27 February 2013, page 2776.
[212] Article 274(1a)(1b) CCP.
[213] Article 274(2) CCP.
[214] Article 274(3) CCP.

measures that need to be taken to protect the professional reliability and whether or not non-public areas may be entered to install the GovWare.[215]

A public prosecutor will ultimately issue an order to the cantonal or federal police. The purchase and use of GovWare is centralised in Switzerland (FDJP, 2019, page 2).[216] One of the interviews shows that the police on the level of the cantons should also be able to apply this authority, but that they lack the necessary knowledge. In practice, the federal police offer GovWare, manage the licences, take care of maintenance and support the various cantons. Also, the federal police act as a liaison for the manufacturer (FDJP, 2019, page 2). If a canton wishes to make use of GovWare and has been granted authorisation for this, this canton pays a monthly amount to the federal police. The exact amounts[217] are specified in Article 3a of the Regulation[218] and the explanatory notes to this regulation. The federal police have eight licences, suitable for eight computer systemcomputer systems, which can be deployed simultaneously (FDJP, 2019, page 4). The federal police collect data with the use of GovWare and then transfer these data to the police team in charge of the criminal investigation.[219]

7.3 Against whom?

The power may be deployed against a suspect,[220] but also against third parties. The latter does come with conditions: 1) the suspect makes use of the postal address of the telecommunications service of a third party;[221] or 2) the third party receives communications on behalf of the suspect or sends the communications from a suspect to another person.[222]

If surveillance is aimed at a person belonging to a professional group as referred to in Articles 170-173 CCP, consider persons bound by professional confidentiality such as lawyers and physicians, any intelligence unrelated to the subject of the investigation is kept secret under the supervision of a judge. The same applies to the reason why that person is being observed. No professional confidential information may come to the Public Prosecution Service's knowledge. The separated data must be destroyed immediately and may not be analysed.[223] Information need not be separated if 1) there is a strong suspicion that the person bound by professional confidentiality has committed a criminal offence;[224] and 2) particular reasons require this.[225] If surveillance takes place of other persons and those persons are in contact with those persons referred to in Articles 170-173 CCP, those communications are then separated in accordance with Paragraph 1. The information on which a person as referred to in

[215] Article 274(4) CCP.
[216] *Erläuterungen zur Revision der Verordnung über Gebühren für Verfügungen und Dienstleistungen des Bundesamtes für Polizei* (*Gebührenverordnung fedpol, GebV-fedpol*) (digitale-gesellschaft.ch).
[217] One month is 13,750 Swiss francs, two months is 27,500 Swiss francs and three months is 41,250 Swiss francs. A separate amount is charged if the deployment is extended (FDJP, 2019, page 4).
[218] AS 2017 245 – *Verordnung über Gebühren für Verfügungen und Dienstleistungen des Bundesamtes für Polizei* (*Gebührenverordnung fedpol, GebV-fedpol*) (admin.ch).
[219] The Dutch police also make a distinction between technique and tactics (Van Uden & Van den Eeden, 2022).
[220] Article 270(a) CCP.
[221] Article 270(b)(1) CCP.
[222] Article 270(b)(2) CCP. According to case law, telecommunication surveillance is also allowed if it is very likely that the third party receives communication from the suspect (BGE 138 IV 232).
[223] Article 271(1) CCP.
[224] Article 271(2a) CCP.
[225] Article 271(2b) CCP.

Articles 170-173 CCP can refuse to testify is separated from the case file and immediately destroyed. That information may not be used.[226]

7.4 Cases

Article 269ter(1b) CCP stipulates that GovWare may be used for criminal offences listed in Article 286(2) CCP. This latter article pertains to infiltration. Paragraph 2 includes an extensive list of criminal offences. It refers to both criminal offences mentioned in the Swiss Penal Code (*Schweizerisches Strafgesetzbuch'* – SR 311.0 – Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (admin.ch)), and criminal offences included in other laws.[227] The Swiss Penal Code mentions for example intentional homicide,[228] murder,[229] misappropriation,[230] computer fraud,[231] trafficking in human beings[232] and participation in a criminal or terrorist organisation.[233,234]

7.5 Time Frame

The Coercive Measures Court initially grants authorisation for a maximum period of three months. Following that period, the deployment may be extended once or several times, each time for a maximum period of three months. No maximum period or maximum number of extensions is agreed. If a public prosecutor wants to extend the deployment, he or she will have to submit an application at the coercive court stating the reasons for the extension. This application must be submitted to the court before the end date of the deployment that had previously been authorised.[235] The moment the conditions for deployment can no longer be met[236] or if no authorisation is given for the deployment or the extension thereof, the public prosecutor directly terminates the deployment.[237] If a situation arises as referred to in Paragraph 1a, the public prosecutor will notify the Coercive Measures Court of the termination of the deployment.[238]

7.6 Formalities

Article 269ter(1a) CCP states that the conditions referred to in Article 269(1)(3) CCP apply to the deployment of this power.[239] Paragraph 1 states that a) there is a strong

[226] Article 271(3) CCP.
[227] For instance, the federal law of 22 June 2001 on the The Hague convention on adoption and measures for the protection of children in respect of intercountry adoption (Bundesgesetz vom 22. Juni 2001133 zum Haager Adoptionsübereinkommen und über Massnahmen zum Schutz des Kindes bei internationalen Adoptione), the Arms Act (Waffengesetz vom 20. June 1997) and the Narcotics Act (Betäubungsmittelgesetz vom 3. Oktober 1951).
[228] Article 111 of the Swiss Penal Code.
[229] Article 112 of the Swiss Penal Code.
[230] Article 138 of the Swiss Penal Code.
[231] Article 147(1)(2) of the Swiss Penal Code.
[232] Article 182 of the Swiss Penal Code.
[233] Article 260ter of the Swiss Penal Code.
[234] In accordance with Article 269ter(1a) CCP, it could be assumed that GovWare may also be used in the case of criminal offences listed in article 269(2) CCP. However, the explanatory notes to the revised BÜPF describe that article 269ter(1a) CCP does not refer to Article 269(2) CCP. This is partly because of the far-reaching nature of the power.
[235] Article 274(5) CCP.
[236] Article 275(1a) CCP.
[237] Article 275(1b) CCP.
[238] Article 275(2) CCP.
[239] Article 269 CCP arranges the surveillance of post and telecommunications.

suspicion of a criminal offence having been committed listed under Paragraph 2 of respective article; b) the seriousness of the criminal offence justifies surveillance; and c) investigation activities thus far conducted have produced no results or would otherwise make the investigation pointless or disproportionately difficult. Paragraph 3 sets out that the surveillance of post and telecommunications may be recommended if the trial of a criminal offence, subject to military jurisdiction, is assigned to a civil court. In addition to these conditions, before proceeding to the use of the power, previous 'traditional' forms must have been unsuccessful.[240] The power can also be deployed if this traditional form of surveillance is useless or disproportionately difficult (Article 269ter(1c) CCP).[241] The power may not extend criminal investigations (*Strafverfahren*) and may not be used preventively.[242] If the public prosecutor issues an order for the deployment of the power, that order needs to contain the following information: the types of data and non-public areas that may need to be entered to install the software on the computer system.[243]

Article 276(1) CCP stipulates that recordings that required authorisation but that are not required for the criminal proceedings must be kept separately from the file and deleted directly after the trial. Article 278 CCP focuses on accidental finds. Amongst other things, it covers how to handle the data collected that pertain to criminal offences other than for which an order had been issued and the circumstances under which these may be used (278(1) CCP). Paragraph 5 stipulates that all findings may be used for tracking down persons who are wanted. It is further regulated that any data collected with the use of software and not included in the order must be destroyed immediately. No use may be made of information from those data.[244] Finally, Article 269ter CCP stipulates that the public prosecutor keeps statistics on the deployment of this power. More about this is regulated in Article 13 of the Ordinance on the Surveillance of Post and Telecommunications ('Verordnung über die Überwachung des Post- und Fernmeldeverkehrs' (VÜPF).[245]

7.7 Technical tools

As previously mentioned, the federal police conduct all activities pertaining to GovWare. One of the interviews shows that the police use both internally developed and commercial tools. Following an order from the public prosecutor, the federal police ensure that the software is installed on the suspect's computer system. This can be done both physically and remotely. Depending on the public prosecutor's order, the software is tuned to (designed for) the suspect's computer system and configurated. During the data collection process, the data intercepted are sent via the suspect's telecommunications connection to the server of the Public Prosecution Service and the police (*Strafverfolgungsbehörden)*.[246] The software must be configurated so that only communication data can be intercepted. This also prevents the possibility of an online search. GovWare must be configurated in such a way that the developer of GovWare has no access to the data if it is used as a technical tool. This also applies to police

[240] Article 269 CCP.
[241] Article 269ter(1c) CCP has similarities with Article 269(3) CCP.
[242] Botschaft 27 February 2013, page 2701; page 2771.
[243] Article 269ter(2a)(2b) CCP.
[244] Article 269ter(3) CCP.
[245] A number of 'standard' conditions also apply to the use of coercive measures in general. These are laid down in article 197 CCP. Paragraph 1b of that article provides, for example, that for the use of a coercive measure there must be a reasonable suspicion that a crime has been committed.
[246] Botschaft 27 February 2013, page 2774.

officers involved in GovWare's management, for example persons managing the server that stores the data obtained using GovWare.

As the software is adjusted to the suspect's device and the software will not be installed on the computer system for a long period of time, it would be very difficult to copy the software and install it on a different device. A third party could therefore not easily misuse the software.[247] If the data collection is terminated, the police make sure to deactivate the GovWare. The latter is not needed if the deactivation process is done automatically.[248] The explanatory notes to the new Act do mention that the experts consulted from the field of science consider that
the software that was to be used cannot yet be restricted to just intercepting communications. Access could be gained to any data held on a computer system.[249]

7.8 Safeguards

7.8.1 Full logging & secure data transfer

During the legislative process, providers and various private individuals expressed their concerns about the quality of the data being collected with the use of GovWare, more specifically about the reliability and integrity of those data, i.e. the possible changes that GovWare makes in documents.[250] In the end, the CCP included a limited number of conditions pertaining to GovWare's quality and the quality of the data collected with the use of this software. Article 269quater CCP describes these conditions. The first condition is that software may only be used that records communications 'unalterably and without interruption'.[251] The second condition involves the secure transmission of data from the suspect's computer system to the police and the Public Prosecution Service (*Strafverfolgungsbehörde*).[252] Regarding both conditions, nothing is specified in the law about how those conditions should be guaranteed and realised. Nor is there a public police guideline that translates these conditions into technical requirements.[253] However, the interviews do make clear that the police test GovWare on the basis of a number of conditions and that measures are taken to securely transmit data, e.g. via hashing and forensic containers.[254] The interviews also indicate that the reports to the public prosecutor explain the working method, including the hashes. Regarding the latter, a person interviewed indicated that the Public Prosecution Service and the courts trust the police. At the same time, it is indicated that if there is any doubt about the evidence presented, the Public

[247] Botschaft 27 February 2013, pages 2774-2775.
[248] Botschaft 27 February 2013, page 2774.
[249] Botschaft 27 February 2013, page 2775.
[250] Botschaft 27 February 2013, page 2773.
[251] Article 269quater(1) CCP.
[252] Article 269quater(2) CCP.
[253] There are various additional laws and regulations for the interception of post and telecommunications, such as the BÜPF, VÜPF, VBO-ÜPF (Verordnung des EJPD über das beratende Organ im Bereich der Überwachung des Post- und Fernmeldeverkehrs), Gebv-ÜPF (Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs), VD-ÜPF (Verordnung des EJPD über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs) and VVS-ÜPF (Verordnung über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs). Except for Article 13 VÜPF, which stipulates that the Public Prosecution Service must keep statistics on the use of GovWare, these additional laws and regulations do not relate to the use of GovWare. Article 13 VÜPF stipulates that the figures must show for which type of crime this power has been used (art. 13, paragraph 1 BÜPF). These statistics will then be submitted to the Post and Telecommunications Surveillance Service. This concerns deployments that have been completed (art. 13, paragraph 2 VÜPF). This service will publish the figures annually. No details are given about the canton of the authority requesting the exercise of the power (Art. 13(3) VÜPF).
[254] They also explain that it is not fully clear for the police what happens when the data leave the device and are sent to the police environment.

Prosecution Service and the judge will want to make sure that the evidence has been collected in a lawful manner. If it turns out that this is not the case, the admissibility must be tested against the principles laid down in Article 140 CCP ('Prohibited methods of collecting evidence', for example threats and the use of force). Article 141 CCP then discusses the admissibility of evidence that has not been obtained lawfully (personal communication, March 31, 2023). For example, evidence collected using force may not be used.[255]

7.8.2 Publication of the source code

The third condition is that judicial authorities must ensure that the source code can be verified so that it can be stated with certainty that the software only has the legally permitted features.[256] In one of the interviews it is explained that commercial suppliers have to confirm in writing that they agree to the dislosure of the source code, if requested by court. As far as known, such requests have not yet been made.

7.8.3 Special service and examination

The original legislative proposal had included two more conditions (Basanisi, 2019, p. 12). The first condition had meant for the Swiss Confederation (*der Bund)* to manage a service that purchases those special IT programs. This service was to be tasked with developing computer programs to monitor communications or to procure these programs from third parties. The second condition was that Examining Magistrates would only be allowed to use programs approved by the Confederation. This implies that the Confederation was to perform examinations. It also meant that the Examining Magistrates would pay a reasonable allowance for the costs of purchasing special programs. Following a decision in January 2016 from the Legal Committee of the National Council on the revision of the BÜPF (*der Rechtskommission des Nationalrates zur Revision des BÜPF)*, these conditions were ultimately excluded from the Act (Basanisi, 2019, pages 12-13). Various arguments played a role in not wanting to include prior certification and the central procurement of GovWare in the law. For example, the committee considered prior certification problematic, because software has to be updated continuously (weekly). This would mean that new certification would be required with each new update and that software that has undergone an update cannot be used immediately. After all, testing will first have to be done in order to achieve certification. In addition, certification would require a lot of time, effort and resources, such as checking several hundred thousand lines of code. Certification would increase the cost of these types of programs several times. In addition, the committee believed that central procurement is problematic, because the question is who is ultimately responsible if GovWare causes damage to a computer system (the federal state or the cantons themselves) (Engler, 2015). Instead, some of these points (development, procurement and costs) were laid down in a regulation (see above).

7.8.4 Other technical and organisational measures

The Federal Department of Justice and Police (FDJP) (*Eidgenössischen Justiz- und Polizeidepartements*) answers a number of questions on its government website on monitoring telecommunications in relation to the quality of the data being collected. To ensure the most secure use of GovWare, the FDPJ indicates that both technical and

[255] Article 141 paragraph 1 CCP.
[256] Article 269quater(3) CCP.

organisational measures will be taken. In terms of technical measures, the police and the Public Prosecution Service (*Strafverfolgungsbehörden)* need to formulate the necessary security features. An independent authority will then check whether they are complete and built in according to recognised standards. In the context of the organisational measures, the police and the Public Prosecution Service will describe a detailed process of the use and operation of GovWare. This includes authorisations and the interaction with the IT system. Furthermore, logging needs to ensure that all steps, from the request to the monitoring process, are traceable, also for the courts (Frequently Asked Questions FAQ | Post and Telecommunications Surveillance Service PTSS (admin.ch)). These abovementioned items are not laid down in law. It is also unclear whether an independent authority was eventually established and the extent to which the other measures such as recording of authorisations and logging, are complied with in practice. There is no public information available about this. In one of the interviews logging is mentioned, but this does not involve technical logging. Instead, it involves logging to show which data have been retrieved, e.g. to show that these were only the data for which the public prosecutor had given permission. The police and the public prosecutor should coordinate what needs to be logged.

7.8.5 Reporting and file

Article 76 CCP has a number of general provisions that must be laid down in writing. This concerns, for example, statements, oral decisions of the authorities and all other procedural acts that are not performed in writing (art. 76 paragraph 1 CCP). This article does not cover police reports. This is regulated in Article 306 DCCP, paragraph 1, which stipulates that the police must establish facts relevant to a criminal offense with the aid of official reports, with the aid of official reports, instructions from the public prosecutor or their own findings. (art. 306 Sv paragraph 1). In its work, the police are guided by provisions relating to investigation, evidence and coercive measures, for example with regard to subpoenas (art. 206 CCP) and arrests (art. 217 CCP). Special provisions of this law are reserved (art. 306 CCP paragraph 3). One of the interviews revealed that after the deployment has ended, the police write a report for the public prosecutor on what has been done in the context of the exercise of the power. Among other things, attention is paid to the fact that data has been retrieved, that it has been stored and that it has been hashed. No information is made public about the exact working method of technical measures (such as GovWare). The report is placed in the file. Furthermore, as a general rule, parties can inspect the file of the criminal proceedings. This is possible at the latest after the first interrogation of the suspect and the collection of other important evidence by the Public Prosecution Service (Art. 101 CCP). It follows from case law that suspects have the right to inspect the recordings of communications so that they can form a picture of how the authorities have selected recordings (Bundesgericht, 2019). Because the hacking power is part of the power to intercept communications, this case law would also relate to data collected by means of the hacking power (personal communication, 1 May 2023).

7.8.6 The notification obligation

Article 279(1) CCP sets out that the public prosecutor notifies a suspect of the deployment of the power, at the latest after the preliminary investigation has been completed. The suspect must be informed of the reason for the use and the nature of the use and its duration. If the Coercive Measures Court agrees to this, the notification obligation may be deferred or dispensed. That is authorised in two cases: 1) if the

findings will not be used for evidentiary purposes;[257] or 2) if postponement or omission of the notification is necessary to protect higher public or private interests.[258] Persons in respect of whom this power has been deployed may object in accordance with Articles 393-397 CCP. The period within which an objection can be lodged starts at the time of notification.[259]

7.9 Case law

As previously mentioned, the number of GovWare deployments must be disclosed annually. In 2020, GovWare was used thirteen times and in 2021 eleven times (FDJP, no date).[260] As far as known, there are no public judgments on cases in which GovWare had been applied based on Article 269ter CCP. One of the persons interviewed indicates being aware of two or three cases in which data had been collected with the use of GovWare and which were to have been accepted, without any discussion. In light of the fact that appeals are pending in these cases, the decisions could not be shared with the researchers. Another interview shows indications of GovWare having been deployed based on Article 280 CCP. However, as far as known, the use of GovWare based on Article 280 CCP has no available case law either.

7.10 In conclusion

Based on Article 269ter CCP, a criminal investigation may involve the use of GovWare to intercept communication data and metadata. This enables the police to gain insight into encrypted communications. GovWare may not be deployed for an online search. Nor would it be allowed to use GovWare for observations, for example, by using GovWare to switch on the camera in a computer system.

The law has laid down three conditions that would add to the quality of the collected data. These conditions relate to the period preceding the deployment, during the deployment of the power as well as after the completion of the deployment. The first condition is that software may only be used that records communications 'unalterably and without interruption'. The second condition involves the secure transmission of data from the suspect's computer system to the judicial authorities. The third condition is that the source code used must be disclosed to demonstrate that the software has no more features than permitted by law. Two conditions were eventually not included in the final version of the law: there will be a separate service that develops and purchases software and Examining Magistrates may only use technical tools approved by the Federation.

In the context of ensuring the quality of the collected data, three issues stand out. First, nothing has been laid down in the law or further supplementary arrangements (such as the order on investigations in computer systemcomputer systems (*Besluit onderzoek in een geautomatiseerd werk*) in the Netherlands) on the actual implementation of these conditions. However, a number of these issues are made more concrete on a government FAQ website. For example, the federal department of the police and the judicial authorities indicates that the police and the Public

[257] Article 279(2a) CCP.
[258] Article 279(2b) CCP.
[259] Article 279(3) CCP.
[260] Statistics | Post and Telecommunications Surveillance Service PTSS (admin.ch).

Prosecution Service must formulate their own security requirements and that an independent authority needs to be set up to monitor those requirements. Other specifications include that authorisations must be recorded and logging must be a requirement. However, there is no public information available about the implementation of these requirements, about whether such an independent authority has been established and/or about whether only use can be made of technical tools that have been approved. In practice, the federal police assess GovWare deployed by them and they determine, in consultation with the Public Prosecution Service, which measures they will take to ensure the quality of the data and what data will be recorded. In that respect, there is confidence from the public prosecutor's office that the police are doing the right thing. There is no case law available at this moment on which basis it could be assessed whether this is indeed the case in the court's opinion (and whether the methods chosen and justified by the police are sufficient).

A second striking issue relates to making the source code available. On paper this seems to be a good method to gain more insight into the exact operation of the GovWare in use. Companies that supply GovWare to the Swiss police were also said to have agreed to making that source code available if the court was to request this. In practice, however, the question is whether that source code would ultimately be made available. Basanisi (2018, pages 14-15) is sceptical about this. He notes that it is problematic that the notion of a source code is left undefined. According to him, proper monitoring is possible only if the source codes of those programs are released that are responsible for both entering as well as monitoring the data installed on the computer system. Basanisi (2019, pages 14-15) also wonders whether source code control is practicable. He has indications that source codes are not made available in practice (Basanisi, 2018, pages 14-15). Previous research by the WODC (Research and Documentation Centre) shows that this is also problematic in practice in the Netherlands. At least one supplier was not prepared to provide insight into the inner workings of the product (Van Uden & Van den Eeden, 2022, page 99). Given the fact that in Switzerland, there is no known case law that relates to cases in which GovWare was used, no definitive answer can be given (as of yet) to the question of whether the source code can actually be made available.

Finally, the third issue relates to the information provision to the suspect and the defence. Switzerland has a notification obligation in which a suspect is informed about the deployment of the power (with possible exceptions). The police also record in an official report any actions taken and any security measures taken. No description is given of the exact operation of the technical tool. In principle, this provision of information offers the suspect's defence to ask questions about the quality of the data. To what extent this actually happens in practice, and whether the defence has sufficient information available to do so, has not become clear in the course of this study.

8 Conclusion

An important catalyst for conducting this comparative law study was the first Report issued by the Inspectorate of Justice and Security, hereinafter: Inspectorate, in 2020, on the basis of which the then Minister of Justice and Security concluded that the deployment of technical tools, their examination and approval did not yet accord with the intentions of the legal framework. Also, the evaluation report on the execution of the hacking power in practice, conducted by the Research and Documentation Centre (WODC), showed a similar outcome. In its response to the first Report of the Inspectorate, the Minister indicated that he would initiate a study into the safeguards for the use of technical tools in other countries. Present report is the result of this study.

The central research question for this study was as follows:

What safeguards govern hacking powers abroad, more specifically the use of technical tools, and how does this compare with the Dutch situation?

Different research methods have been used to answer the research question: document studies (laws and regulations and relevant (grey) literature), written questionnaires and interviews. Based on these different research methods, a wide-ranging inventory was made of a large number of European countries and Australia, Canada and the United States. Five countries – Belgium, Germany, France, Sweden and Switzerland additionally underwent a more in-depth analysis. The Dutch situation had already been analysed in the context of the abovementioned evaluation of the hacking power in practice.

This conclusion compares the five countries subjected to in-depth analysis with each other and with the Netherlands. Section 8.1 first briefly focuses on the main issues and bottlenecks faced by the Netherlands in examining the technical tools. Next, Section 8.2 addresses a number of general observations with regard to the other countries, based on the wide-ranging inventory. Section 8.3 compares the countries that had been analysed in more detail. Section 8.4 has concluding remarks in which we explore a number of scenarios that deal with (additional) safeguards with respect to the quality of the data obtained by means of hacking operations. These scenarios are based on the manner in which the different countries approach the hacking power.

8.1 Main issues and bottlenecks in examining technical tools in the Netherlands

For the introduction of the hacking power, the Dutch legislator opted to follow the examination system of technical tools already set in place for existing (special) investigative powers. A separate decision was prepared for the authorised hacking titled 'the Decision on intruding into automated information systems (hacking)', hereinafter: the Decision. The Decision sets a number of requirements for technical tools, including requirements aimed at integrity, traceability and reliability of the data collected, hereinafter: quality. The Dutch National Examination Service is tasked with examining the tools in the Netherlands, thereby applying an examination protocol based on various articles from the Decision. In principle, the police must make use of technical tools that have been examined and approved prior to their use. This is

subject to a number of exceptions: 1) a technical tool may be examined afterwards, 2) it is possible to switch to manual deployment or 3) the public prosecutor decides that the tool cannot be examined 'on account of its nature'.

The Reports from the Inspectorate (Inspectorate of Justice and Security, 2020; 2021; 2022) and the first evaluation report from the Research and Documentation Centre (Van Uden & Van den Eeden, 2022) show that the examination and the use of technical tools do not always proceed as intended by law. Pre-approved technical tools are hardly ever deployed, and examination is a major bottleneck for investigation practices. Different aspects play a role here (Van Uden & Van den Eeden, 2022, pages 131-147):

- The turnaround time of an examination takes a relatively long time, at least four months. That timeframe does not always match the promptness that may be required within an investigation.
- Adjusting a technical tool that has not been approved yet always required a new examination and thus takes time.
- The Decision demands, and consequently so does the Dutch National Examination Service, that technical tools must meet all requirements for the technical tool to be approved. Investigation practices, however, question the usefulness and necessity of all requirements and the compliance thereof.
- The deployment of technical tools takes place in an environment which Digit, the police team executing the power, cannot always control. For example, Digit cannot exercise any influence over what suspects do with their computer systems. Any action from the owner of the automated computer system can affect the quality of the data collected. Digit would prefer to focus more on making risk analyses with regard to the technical tool used and the evidential value of the data collected.
- A risk analysis focuses on the risk of data quality being compromised if a technical tool is used that does not meet all requirements.
- Another consideration is the impact of using a technical tool that does not meet all requirements on the evidential value of the data collected. Especially, if the data only form part of the evidence collected.

The majority of police investigations in which hacking operations are carried out make use of a commercial product. Here, too, no pre-approved tools were used. In fact, the products were never submitted for examination, because the Digit public prosecutor decided that the nature of the tools preclude an examination. In so doing, the public prosecutor makes use of the Decision's ground for exception. Incidentally, these products can indeed not be approved under the current examination regime. There are a number of factors that make a commercial tool inherently impossible to approve and/or never to be approved (Van Uden & Van den Eeden, 2022, pages 134-147):

- Commercial tools are updated relatively often. The question then becomes, which version or versions should the Dutch National Examination Service approve? If all the versions need to be approved, it would exceed the usual lead time needed for examination and approval in relation to the timeframe within which the police action must take place.
- Operation of these types of tools is a 'black box' for the users, which is why the Dutch National Examination Service is not given access to the exact operation and can therefore not carry out a full inspection.
- Suppliers want to have access to their product at all times, to do things like perform maintenance, for example. As a result, the Dutch National Examination Service is not given exclusive access to the tool, which it requires for its examination. Not having exclusive access means no approval, as it cannot be ruled

out that a party other than the suspect and the police had access to the data collected. This means that the reliability and integrity of the data cannot be fully guaranteed.

Failing to perform the examination means that a majority of criminal investigations do not comply with a key safeguard with regard to the quality of the data collected. It should be noted, however, that additional technical and tactical safeguards are put in place in this situation to ensure the reliability of the evidence. These tactical safeguards are not included in the examination.

8.2 General observations in other countries

Our general inventory shows that the emphasis of the legal framework in other countries lies on the legitimacy of the hacking power. Most of the safeguards relate to the proportionality of the power. These include:

- The types of criminal offences for which the hacking power may be deployed.
- The hacking power's purpose limitation: is the authorised hacking used for the legal purposes for which it may be deployed?
- The investigative actions that may be performed with the use of authorised hacking.
- The period of the hacking power's deployment.
- The hacking power's impact if deployed in the suspect's computer system: to what extent does the deployment of the technical tool temporarily or permanently affect the operation or security of the computer system.

Incidentally, this is not to say that additional safeguards may not otherwise be present in these countries. For instance, the police may apply internal policy rules. As far as we could ascertain, these are not publicly available, making it formally unknown what those exact rules are. However, it did become clear in our research that in many countries, the actions carried out by the police have to be reported and explained, should a session judge hear the case. So while we have not been able to gain full insight into the contents of the policy rules put in place within the police forces in the different countries, it does seem plausible on the basis of the inventory that the police will adopt certain best practices to demonstrate the legitimacy and evidential value of the data obtained.

In the course of our research, we found hardly any case law that discussed the quality of the data collected with the help of hacking operations. This unfortunately does not provide any further clarity on whether or not best practices are applied and how a session judge values them. It should be noted though that the fact that there is no case law does not mean that the quality of the data has not been called into question, only that it has not found its way into court decisions. Based on their own experience, interviewees said they knew of very few cases where data quality was called into question. They expect that this will occur more frequently in the future. According to the interviewees, the fact that this has not happened yet could be partly due to the fact that the hacking power is relatively new, due to a lack of technical knowledge on the part of the defence and/or the additional (conclusive) evidence presented.

8.3 Comparison between countries

Our study examined five countries in more depth: Belgium, Germany, France, Sweden and Switzerland. The underlying subsections compare these countries with each other and with the Netherlands. This is done with regard to safeguards prior to the deployment, during the deployment and after the deployment of the hacking power. The focus is placed on the most notable issues.[261]

8.3.1 Safeguards prior to the deployment of the power

Table 8.1 provides an overview of the safeguards that apply prior to the deployment of the hacking power, thus before an automated computer system is hacked.

Table 8.1 Overview of the safeguards prior to the deployment of the power

Country	Safeguard
Belgium	The police test the technical tools themselves based on internal confidential rules.
Germany	A technical tool should be installed in such a way that it only records ongoing communications or the contents and circumstances of the communications.
	No alterations may be made to the automated computer system unless strictly necessary.
	Suppliers need to comply with specified requirements, which the software user or a designated authority assesses. The SLB guideline serves as a guiding principle for this assessment. Part of the assessment is a risk analysis of the technical tool and the environment.
	Government organisation ZITiS can assist in the procurement of technical tools and the assessment as to whether these tools comply with the legal framework. However, this is not a formal examination. Going forward, the plan is for the organisation to also develop in-house technical tools.
France	The government service STNCJ is responsible for the implementation of technical tools and for the execution of the hacking operations. It is not known what criteria it uses for procurement and assessment of the tools.
The Netherlands	Prior to a deployment, the Dutch National Examination Service monitors whether a technical tool meets all the requirements on the basis of an examination protocol. This protocol is based on various articles from the Decision.
	In principle, technical tools can only be deployed if approved by the Dutch National Examination Service. There are a number of exceptions to this principle: retrospective examination, a manual deployment and the tool cannot be examined 'due to its nature'.
Sweden	Features of a technical tool are limited to fit the contents of the order.
	A technical tool may not cause unnecessary damage.
	Standardised software and tools from other police forces may be used.
Switzerland	Features of a technical tool must be limited and only serve the interception of communications.

[261] As previously noted, it is unclear what the police's internal policy rules entail. It is therefore possible that countries have more safeguards than those discussed in the following sections.

Country	Safeguard
	There is restricted access to data: a *GovWare* supplier is not allowed access to data.
	The police test the technical tools themselves based on internal confidential rules.

Except for Sweden, all countries have some form of examination or testing of the technical tool to be used. However, the manner differs per country. The Netherlands has the most detailed *described* examination of technical tools. The manner in which Germany has described the criteria appears closest to the way the Netherlands has done this. The German examination is based on the SLB Guideline,[262] which highlights the following themes: protection targets and security measures, work processes and procedures, suppliers, and test policy. Application of the guideline serves as a guiding principle; it is not a legal requirement. A risk analysis is used to identify which objects, e.g. system components such as hardware and software, applications, organisational or personnel issues, pose a risk for these themes. The results of this risk analysis, the determination of the protection needs and the resulting consequences and implementation thereof are laid down in an IT security concept. Both software suppliers and users of the software must conform to this concept. It is not known what criteria comprise the examinations or tests in the other countries.

The Dutch National Examination Service carries out the examination in the Netherlands. The Dutch National Examination Service is an independent body, though it formally falls under the same organisational unit of the National Police Board to which the team carrying out the hacking operation belongs. In France, the testing is done by a specific government body called STNCJ. This government body is also responsible for the execution of the hacking power. In both countries, the way in which the tasks are assigned may raise the question of how independent the examination is. This applies in particular to France, where it is actually the same organization that carries out the power and inspects the tools. The other countries have the police doing their own testing. It is interesting to note that both in France and Switzerland, the 'inspector' and the 'performing party' are one and the same party. These countries do not consider this to be problematic and proceed on the assumption that the parties act in a fundamentally trustworthy manner. As far as known, there is no formal examination in Sweden. However, they often use standardised software at a later stage of the hacking process, i.e. once the data are placed on the police's systems. This standardised software, for example, involves software that has been certified by other police services such as the Dutch police.

8.3.2 Safeguards during the deployment of the hacking power

Table 8.2 provides an overview of the safeguards that apply during the deployment of the hacking power, i.e. the period during which there is access to an automated computer system and the data is being retrieved.

[262] In full '*Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung*'.

Table 8.2 Overview of the safeguards during the deployment of the power

Country	Safeguard
Belgium	Every five days, the police submit a written report to an examining magistrate. The examining magistrate may decide to terminate the deployment.
Germany	According to the state-of-the-art, technical tools must provide protection against unauthorised use by third parties.
	The SLB guideline has established criteria in relation to the technical tools that are to be used.
	Copied data must be protected against any amendments, unauthorised deletion and unauthorised access by third parties, according to the state-of-the-art.
	Any updates of technical tools must be installed instantly.
	The data collection must be logged and documented.
	The reporting needs to address the following items: name and time, identification of the automated computer system and any alterations made, information used to record data and the unit carrying out the hacking operations.
France	The authorised hacking takes place under the supervision of the magistrate who authorised that hacking power.
	The STNCJ is responsible for the storage of the data obtained.
The Netherlands	All investigative actions must be logged during the deployment.
	The transport of data of the automated computer system to the police's technical infrastructure has to take place in a secured and encrypted manner.
	The data obtained is stored on a secure police infrastructure.
	Oversight by the Inspectorate may take place during deployment.
	The reporting needs to include the following: any irregularities, placement of the technical tool, execution of the investigative actions, erasing of the technical tool, incomplete erasing of the technical tool and a selection of data, if processing of data has taken place.
Sweden	Internal policy rules (not publicly available).
Switzerland	Data logging has to be done invariably and uninterruptedly.
	The transport of data between the automated computer system and the police's systems must be done in a secure manner.
	The police have to draw up a report on the actions performed.

The safeguards that must be in place during deployment of the hacking power differ per country. Common safeguards at this stage are forms of logging, reporting, the use of a secured transport of data from the automated computer system and the storage of data in a secured environment. Although there are no safeguards listed in this table for Sweden, it is known that the Swedish police apply internal policy rules that include different safeguards. However, these policy rules are not publicly available.

There is judicial review in Belgium and France during the hacking operations. The judge granting authorisation for the deployment of the hacking power also supervises the execution thereof. If the execution of the hacking power does not take place in accordance with the conditions of the authorisation, the hacking operations may be terminated. It should be noted in this respect that the judge relies on the information

that the police or the public prosecutor provides or may provide during the deployment. The question is thus whether this judicial oversight will actually ensure that a deployment can be terminated mid-term. The judicial oversight in these countries goes beyond the role of the Examining Magistrate in the Netherlands, who principally only oversees the hacking power prior to a deployment or its extension. However, the Netherlands still has the supervision by the Inspectorate of Justice and Security.

8.3.3 Safeguards after the deployment of the hacking power

Table 8.3 provides an overview of the different safeguards in terms of the period after the deployment of the hacking power. This refers to the moment when the police no longer have or may no longer have access to the automated computer system and data are no longer being collected.

Table 8.3 Overview of the safeguards after the deployment of the power

Country	Safeguard
Belgium	Notification has to be made about the nature and duration of the deployment. Notification cannot in principle be omitted unless the suspect's identity or place of residence cannot be reasonably ascertained.
	The investigating judge decides what selection of information is important for the file. All documents that have been used in the investigation but not added to the case file are either destroyed or sent to the court registry in a sealed manner. The defence may request the investigating judge to add information to the case file.
Germany	If technically feasible, the modifications made to the automated computer system must be undone automatically after the deployment of the power has ended.
	Notification has to be made of the hacking operations. Notification may be deferred or eventually omitted subject to conditions.
	The software used must be archived.
	The defence may call the software's quality into question based on the data they receive.
France	A data subject will only be notified if the case is brought before the court. There is no notification obligation.
	A transcript of the data is provided at the hearing but no further information is given as to its origin and how the data were obtained. In special cases, the lawyer may request to declassify information. If a session judge complies with that request, the defence may be provided with more information.
The Netherlands	A data subject needs to be notified after the hacking operations have taken place. The notification may be deferred.
	The Inspectorate of Justice and Security may supervise the execution of the hacking power both during and after the deployment.
	After completion of the police action, the technical tool will be erased to the extent possible.
	The suspect will be given access to the data in evidence on file. The defence may submit a reasoned request to access additional data.
Sweden	A notification must include the following information: the type of power deployed, the deployment's duration, the computer systems that have been hacked and the

Country	Safeguard
	locations. Notification may be omitted for specific criminal offences if investigative interests are compromised.
	The defence may submit a reasoned request for all data collected. Both parties may consult an external expert.
	No information will be disclosed during the hearing about the operation of technical tools.
	The technical tool should be removed after use and the security of the automated computer system should be at least at the same level as before the tool was deployed.
	The Commission on Security and Integrity Protection (SIN) supervises the deployment of the power, something which is principally done afterwards.
Switzerland	The notification has to focus on: the reason, the nature and the duration of the deployment. If the Coercive Measures Court consents to this, the notification obligation may be omitted.
	The suspect may be allowed access to the recordings.
	The source code of the technical device should be verifiable if the court so requests.
	The technical tool has to be deactivated after the deployment.

The most common safeguards pertain to the notification of the deployment of the hacking power to the suspects or the data subjects, the substance of the case at the hearing and the suspect's right to inspection. Notification is not a guarantee in all countries, given that such notification may be omitted if it could compromise ongoing interests of the investigation. The law in Belgium always requires notification. France is the only country in which a suspect does not need to be notified. It goes without saying that if the data hacked form part of the evidence, the suspect is indirectly notified by the inspection of the file. Not all countries have made it clear what information is included in the file, and to what extent the right to inspection extends. However, it does emerge that in most cases the defence receives a copy of the data collected by means of hacking operations or a collection thereof.

As previously noted, there is still little case law available that calls into question the quality of the data collected by means of hacking operations. This makes it difficult to answer the question of how extensively a session judge assesses the deployment and the data quality. The case law that is available mostly deals with cases where evidence is used based on data from the Encrochat communications service. The French authorities have been able to intercept these communications. Many countries have used Encrochat data as evidence. However, the main issue in these cases was whether this was legally obtained evidence rather than the quality of the data collected. As far as known, the quality of data has only been called into question in Sweden and France. In Sweden, the court dismissed relatively easily the objections raised regarding data quality. The court added that the data, in conjunction with other investigation data, show that 'the messages correspond well to the reality in terms of time and content'.[263] More striking is an October 2022 ruling from France.[264] In this ruling, the court concluded that in the absence of a certificate of truthfulness, it cannot be

[263] Judgment given by Stockholm District Court on 22 April 2021 in case no. B 5546-20, page 9.
[264] The French Supreme Court, criminal division, 11 October 2022, appeal no. 21-85.148.

accepted that nothing is shared about how the evidence was obtained. However, this only applies if the collected data is encrypted. It is likely that the police use the authority to view decrypted messages (live). Therefore, in these cases a certificate is not required.

Another striking issue in terms of the safeguards at the end of deployment is the legal provision applicable in Switzerland that stipulates that it must be made possible to check the source code of the technical tool if so requested by the court. Prior to deployment, it must also be ensured that the supplier cannot access the data. Source code disclosure and access restriction stand out because both issues are a major obstacle in the Netherlands to examining and approving commercial tools. A relevant question, which unfortunately cannot be answered based on our research, is thus to what extent both requirements can ultimately be enforced in Switzerland.

Finally, it is worth noting that Sweden is the only one of five countries that has a specific supervisory body (SIN) that monitors the hacking power. SIN's role in relation to the use of technical tools for the hacking power is still evolving. For the time being, supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness. However, SIN also has the authority to check the technical tools themselves. While SIN's rulings are not binding, authorities generally follow SIN's rulings. SIN has partly similar tasks to the Inspectorate in the Netherlands, but it additionally oversees the lawfulness of the entire process and thus also the activities of both the police and the public prosecutor. SIN can furthermore issue public statements in individual cases. The suspect may also personally request this.

The foregoing has shown that the Netherlands has established a very detailed examination process compared to other countries. Our inventory shows that four out of five countries test technical aids before they are purchased and deployed. However, it is unclear how far-reaching this test is and to what extent the quality of data plays an important role in this test. Furthermore, the focus of the guarantees in these countries lies in the final phase of the use of the authority. After the power has been used, the quality of data can be brought into question during the hearing. In the Netherlands, the examination must in principle ensure that the quality of the data obtained is not called into question.

8.4 Concluding remarks

Based on our research, we have formulated three scenarios which could potentially complement the way in which the Netherlands deals with technical tools and data collected by means of the hacking power. These scenarios are described in the text below.

Scenario 1: Source code and monitoring data access
Our research shows that it is required by law in Switzerland that it must be made possible to check the source code of the technical tool if so requested by the court. It must also be ensured that suppliers cannot access the data when these are being collected. These issues specifically form an obstacle in the Netherlands in inspecting commercially technical tools. It has not become clear to what extent the Swiss authorities have actually been able to fulfil both requirements. As far as is known, there has not yet been a case in which the source code was actually requested. In principle, suppliers do not benefit from giving access to their source codes. The

software's working method is a well-kept secret. However, if Switzerland has succeeded in finding a workable solution, it is worth considering whether the police, public prosecutors and policymakers in the Netherlands can also achieve this in a similar manner. This could resolve two major bottlenecks in the examination procedure in the Netherlands.

Scenario 2: Changing supervisory role
Supervision during the deployment of the hacking power has been a key topic of discussion throughout the Dutch legislative process. Additional oversight was considered to be essential because courts would not always be capable of properly assessing the evidence collected. It was also expected that a (major) part of the cases would never be brought before a court. It has been suggested to set up a body similar to the Review Committee on the Intelligence and Security Services (CTIVD). Different authors (consider Hildebrandt, 2016; Buruma, 2016; Schermer, 2017) advocated in previous years that this body should 'also expressly assess the lawfulness of the data processing by the police headed by the Public Prosecution Service in the investigative process' (Oerlemans, 2018, page 18-19). Fedorova and colleagues (2022) reach a similar conclusion in their report. Hirsch-Ballin and Oerlemans (2022) assert that the current oversight system for data-driven investigations is lacking and also suggest the establishment of such a supervisory body. The purpose of this supervisory body would be to enforce the Directive on data protection in criminal investigations and prosecutions, as well as play a supervisory role in a broader sense in relation to data-driven investigations (Hirsch-Ballin and Oerlemans, 2022, page 12). Also, the report of the 'Committee on Modernisation of Criminal Investigations in the Digital Age' (Commissie modernisering opsporingsonderzoek in het digitale tijdperk; Koops Committee) focuses on supervision. It offers recommendations to 'specifically address the longer-term sustainability of the supervisory system, as well as the setup of external oversight of the data collection and data processing by investigative services' (Koops Committee, 2018, page 31). However, the Committee did not mention any specific measures, such as the establishment of a separate committee modelled on the CTIVD. Ultimately, the establishment of such a committee was not chosen (Van Uden & Van den Eeden, 2022, pages 206-207). Arguments for this included the Examining Magistrate's oversight already in place and the supervision by the Central Assessment Committee of the Public Prosecution Service (*Parliamentary Papers II 2015/16, 34 372, no. 4, page* 20). Instead, the choice went to the Inspectorate of Justice and Security, overseeing cases that are or are not presented to court (Van Uden & Van den Eeden, 2022, page 207).

Based on our research, we do not take a position on this discussion. However, it is worth noting that if the role of oversight for hacking power is explored further, there are a number of countries that have surfaced from the study that may provide guidance.

Firstly, it is relevant in this context that Belgium and France have examining magistrates overseeing the execution of the hacking power. The Examining Magistrate granting authorisation for the deployment of the hacking power also supervises the execution thereof. If needed, the Examining Magistrate may decide to terminate the hacking operations. This oversight goes beyond the role of the Examining Magistrate in the Netherlands, who principally only oversees the hacking power prior to deployment. The working method in Belgium and France solves the problem that part of the cases are not presented to court. As a side note, it should be noted that the examining magistrates rely on the information provided. The question is thus whether this judicial

oversight actually results in a substantive review during deployment. It does however offer a perspective that deviates from the Dutch system in which the Examining Magistrate grants an authorisation prior to the deployment and thereafter generally no longer oversees the hacking operations.

Secondly, also relevant is the Swedish supervisor SIN. This supervisor specifically oversees the execution of the hacking power. It is therefore similar to the Committee modelled on the CTIVD as proposed by some authors. As yet, SIN's supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness and it oversees both the police activities as well as those of the Public Prosecution Service. As such, it distinguishes itself from the tasks of the Inspectorate in the Netherlands, which only oversees the police. SIN can furthermore issue public statements in individual cases upon request or on its own accord. Given that SIN focuses both on the legal and process-related aspects, this solves the issues raised earlier that not all cases are heard by a session judge and that the judge is not always sufficiently capable of properly assessing the evidence.

Scenario 3: Customised examination

As previously discussed, the examination in the Netherlands constitutes an important safeguard in the deployment of technical tools and the quality of the data collected by means of the tools. Practice shows that the examination and the use of technical tools do not always proceed as intended by law. Technical tools that are mainly used are tools that are not pre-approved and technical tools that cannot be approved due to their nature. Notably, the safeguards relating to technical tools and the data quality are less detailed by law abroad than in the Netherlands. In that respect, it is easier to deploy the hacking power abroad. Another striking aspect is that there is little or no case law available that challenges the use of the hacking power in these countries. This incidentally does not mean that the evidence provided by the hacking power will always be readily accepted. In many countries, the hacking power is relatively new and its use and any opinions thereof will continue to develop. Therefore, it cannot be ruled out that future rulings may still ensue that will impact the current legal framework in these countries. This does not detract from the interesting fact that several countries have chosen not to check data quality in a way that is done in the Netherlands. And that the working method in those countries has, as yet, not resulted in any fundamental discussions in the courts. It is for this reason that we have included a third scenario which takes a more tailor-made approach to the examination requirements, with attention to additional tactical and technical safeguards. This scenario explores a) the use of a risk analysis for the examination and b) the question to what extent additional tactical and technical measures are adequately safeguarded.

Scenario 3a: Risk analysis in the examination phase

Risk analyses form part of the decision to purchase and use technical tools in Germany. An SLB guideline addresses various themes that should be taken into consideration when it involves technical tools, such as the examination policy. A risk analysis identifies which objects pose a risk for these themes and what additional measures are needed. The different parties involved must conform to this. In the Netherlands, the performing party Digit indicates that the Dutch National Examination Service, as well as the underlying examination protocol, does not take sufficient account of the fact that it could also operate on the basis of a risk analysis, namely in terms of the measures it takes when deploying a technical tool. It is particularly this risk analysis that appears to have taken centre stage in Germany. Therefore, the

working method in Germany could be further explored to see what lessons can be learned from it in terms of the Dutch situation.

Scenario 3b: Assurance of additional tactical safeguards in the Netherlands
As noted, the Netherlands currently mainly uses technical tools that, according to the Public Prosecutor, cannot be approved due to their nature. Tactical and technical measures are taken to safeguard the data quality in this situation. There are no indications at present that the use of commercial products will be terminated. The current Minister considers this to be a 'reality that we have to deal with', as evidenced by the committee debate on 7 July 2022.[265] The use of risk analyses described in scenario 3a may serve as a guideline to take appropriate additional measures to ensure data quality. If the working method with commercial products remains the rule rather than the exception and the method will be continued by exactly the same token, it will also be important to review the role of the Public Prosecution Service with regard to the additional safeguards, tactical or otherwise. At present, the Public Prosecution Service is the only one checking these safeguards prior to a deployment. A tactical public prosecutor leading the criminal investigation is in principle ultimately responsible for the tactical safeguards. These are also reviewed by the Digit public prosecutor and the Central Assessment Committee of the Public Prosecution Service. Owing to the sole involvement of the Public Prosecution Service and no other independent bodies, it is useful to explore which other party can (additionally) verify the adequacy of these measures, especially when a case is not presented to court.

In conclusion
For many countries, authorised hacking is a relatively new power. Also, the digital expertise required for the hacking power is relatively new to many parties concerned. As a consequence, legislation and regulations do not always correspond to practice. In the Netherlands, we see this reflected in the bottlenecks related to the examination process. In other countries, we can imagine tightened data quality laws and regulations in the future, possibly driven by case law calling data quality into question. The timeframe for this is uncertain as yet.

The current regulations create bottlenecks in Dutch operational practice, especially with regard to the examination of technical tools. Contrary to the legislator's intentions, few, if any, technical tools are deployed that have been approved prior to their deployment. This applies both to commercial tools and tools developed in-house. Due to the nature and added value of these technical tools, this situation is likely to persist for the time being. To ensure the quality of data obtained with these tools, it makes sense to explore additional measures that can be taken. The scenarios that we have outlined can serve as a guideline for this.

[265] *Parliamentary Papers II* 2021/22, 29 628, no. 1122, page 33.

Samenvatting

De hackbevoegdheid in het buitenland

Een rechtsvergelijkend onderzoek naar wettelijke regelingen en waarborgen omtrent de kwaliteit van gegevens

Op 1 maart 2019 is de Wet computercriminaliteit III (CCIII) in werking getreden. Een onderdeel van deze wet is de introductie van de 'hackbevoegdheid' van de politie. Op basis van de nieuwe artikelen 126nba, 126uba, 126zpa in het Wetboek van Strafvordering (Sv) wordt het voor daartoe geautoriseerde opsporingsambtenaren onder bepaalde voorwaarden mogelijk om op afstand heimelijk binnen te dringen in een geautomatiseerd werk en daarin onderzoek te doen. De onderzoekshandelingen kunnen worden verricht met een technisch hulpmiddel. In beginsel moet een technisch hulpmiddel voorafgaand aan het gebruik ervan worden gekeurd en goed bevonden worden door een onafhankelijke keuringsdienst (de Keuringsdienst), om de betrouwbaarheid, herleidbaarheid en integriteit van het bewijs te borgen.

De Inspectie Justitie & Veiligheid (hierna Inspectie) houdt toezicht op de uitvoering van de hackbevoegdheid. In haar eerste Verslag in 2020 concludeerde zij dat de inzet van technische hulpmiddelen bij de hackbevoegdheid en de keuring van deze hulpmiddelen nog niet verliepen zoals volgens het wettelijk kader was bedoeld. In zijn reactie op het eerste Verslag van de Inspectie heeft de toenmalig minister van Justitie en Veiligheid aangegeven dat hij zou laten onderzoeken met welke waarborgen het gebruik van technische hulpmiddelen in het buitenland is omkleed. Onderhavig rapport is het resultaat van dit onderzoek. Dit rapport vormt tevens een aanvulling op de eerder verschenen evaluatie naar het gebruik van de hackbevoegdheid in Nederland, uitgevoerd door het WODC.

Vraagstelling

De centrale onderzoeksvraag van dit onderzoek is als volgt:

Met welke waarborgen is in het buitenland de hackbevoegdheid, meer in het bijzonder het gebruik van technische hulpmiddelen omkleed en hoe verhoudt zich dat tot de Nederlandse situatie?

De centrale onderzoeksvraag wordt beantwoord aan de hand van de volgende deelvragen:

1 Welke landen kennen een 'hackbevoegdheid' en op basis van welke wettelijke grondslag kunnen buitenlandse politiediensten in hun eigen land gebruik maken van de hackbevoegdheid?
2 Welke wettelijke voorwaarden gelden er in het buitenland voor politiediensten om de hackbevoegdheid in te kunnen zetten?
3 In hoeverre kennen andere landen een keuring van technische hulpmiddelen en wat is hierover in wet- en regelgeving vastgelegd?

4 In hoeverre gelden er nog andere regels om de betrouwbaarheid, herleidbaarheid en integriteit van de gegevens, die zijn verkregen met behulp van de inzet van technische hulpmiddelen, te waarborgen?
5 Hoe verhoudt de werkwijze in het buitenland zich tot de Nederlandse manier van werken met betrekking tot het keuren van technische hulpmiddelen en eventuele andere waarborgen om de betrouwbaarheid, integriteit en herleidbaarheid van gegevens te realiseren?

Methoden van onderzoek

Voor het onderzoek is een brede inventarisatie gemaakt om in kaart te brengen welke landen een wettelijke hackbevoegdheid kennen. Om van een hackbevoegdheid te kunnen spreken hanteerden we als uitgangspunt dat de hackbevoegdheid heimelijk en op afstand wordt uitgevoerd. In het kader van de brede inventarisatie zijn nagenoeg alle Europese landen bekeken plus de Verenigde Staten, Canada en Australië. Op basis van de brede inventarisatie is een selectie van vijf landen gemaakt die nader zijn bestudeerd: België, Duitsland, Frankrijk, Zweden en Zwitserland.
Om de onderzoeksvragen te beantwoorden zijn verschillende onderzoeksmethoden gebruikt: documentstudie (wet- en regelgeving en relevante (grijze) literatuur), schriftelijke vragenlijsten en interviews.

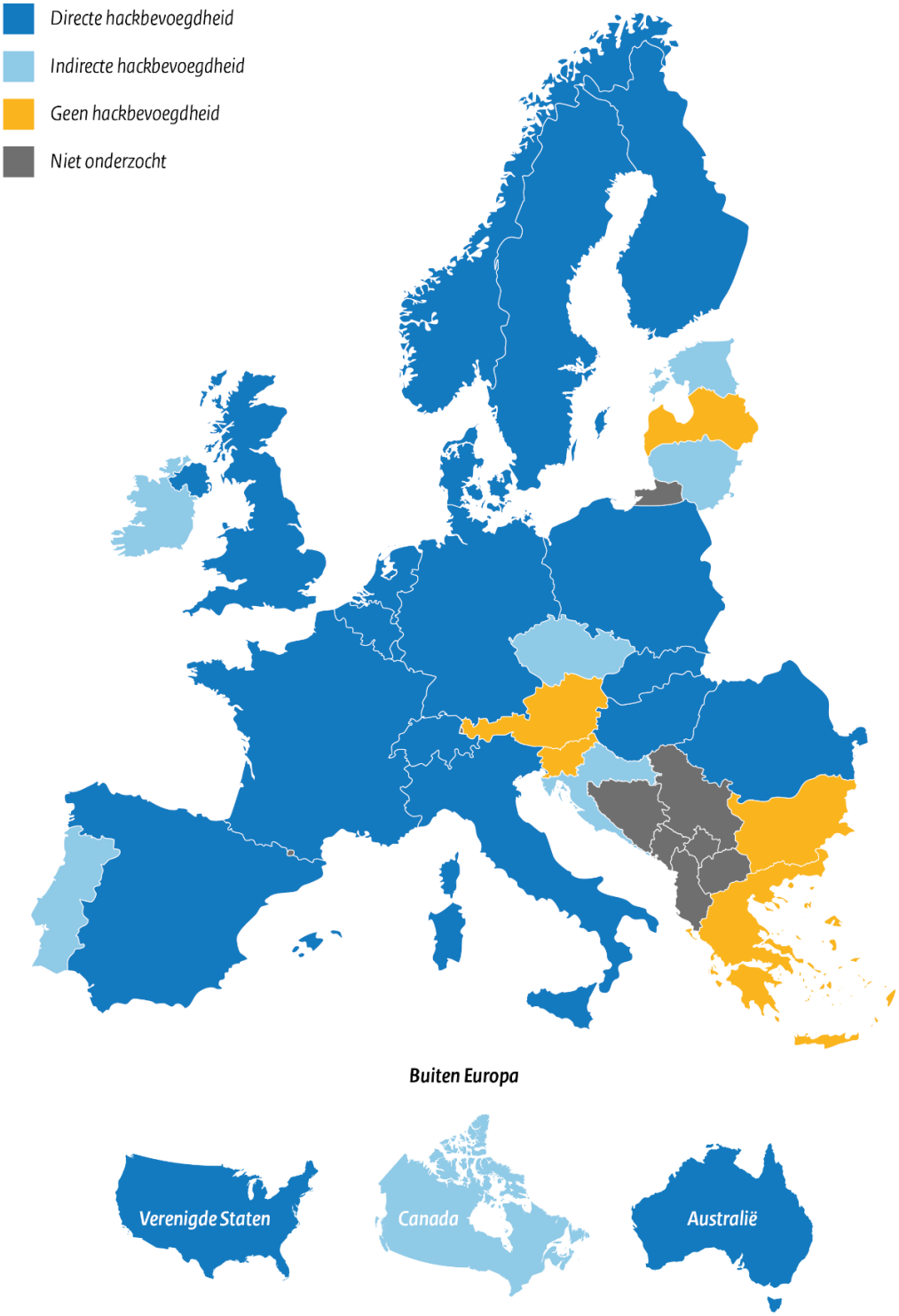
Brede inventarisatie

Op basis van de brede inventarisatie is in dit rapport een aantal onderwerpen besproken. In deze samenvatting wordt aandacht besteed aan de aanwezigheid van een hackbevoegdheid, de keuring van technische hulpmiddelen en de aanwezigheid van een controlerende instantie, de waarborgen voor documentatie, opslag en rechterlijk toezicht, en de notificatieplicht en het inzagerecht.

Aanwezigheid hackbevoegdheid

Het figuur op de volgende pagina geeft weer of een land een wettelijke hackbevoegdheid voor de politie kent en zo ja, of dit een directe of indirecte bevoegdheid is. Van een directe bevoegdheid is sprake als de wet expliciet de mogelijkheid noemt een geautomatiseerd werk heimelijk en op afstand binnen te dringen en daarbinnen één of meerdere onderzoekshandelingen te verrichten. Van een indirecte bevoegdheid is sprake als de hackbevoegdheid deel uitmaakt van een algemene bepaling. Dit gaat bijvoorbeeld om een interceptiebevoegdheid, waarbij in de wetstekst niet specifiek de hackbevoegdheid wordt genoemd, maar de bevoegdheid wel voor dat doel kan worden gebruikt.

Landenoverzicht hackbevoegdheid



Kaarten zijn bewerkingen van werken van Maix (Europa; CC BY-SA 3.0), Theshibboleth/Lokal_Profil (VS; CC BY-SA 2.5), Paul Robinson/Lokal_Profil (Canada; publiek doMayn) en Rycherr (Australië; CC BY-SA 4.0 en eerdere versies).

Keuring technische hulpmiddelen en controlerende instantie

Geen enkel land kent een keuring door een onafhankelijke keuringsdienst waarbij deze keuringsdienst voorafgaand aan een inzet, aan de hand van een uitgebreid keuringsprotocol, de technische hulpmiddelen dient te onderzoeken. Sommige landen kennen wel een testprocedure, maar dit wordt niet uitgevoerd door een onafhankelijke keuringsdienst. Verder geldt voor de overige landen die een keuring of testprocedure kennen, dat onbekend is hoe de procedure eruitziet. Duitsland vormt hierop een uitzondering. Ook daar is niet volledig duidelijk hoe de keuring eruitziet, maar het is wel bekend dat deze gebaseerd is op een speciaal daarvoor geformuleerde SLB-richtlijn.

Het toezicht op de uitvoering van de bevoegdheid door een onafhankelijke instantie is in het buitenland beperkt (de zittingsrechter buiten beschouwing gelaten). Voor Australië, Denemarken, Noorwegen, het Verenigd Koninkrijk en Zweden geldt dat een vorm van toezicht plaatsvindt op de uitvoering van de bevoegdheid door een onafhankelijke instantie. Daarnaast bestaat in Duitsland een instantie die, vanwege haar technische expertise, adviseert over de inzet en ontwikkeling van technische hulpmiddelen. Frankrijk kent een specifieke instantie die verantwoordelijk is voor het ontwerp, de aansturing en de implementatie van technische hulpmiddelen die gebruikt worden voor de hackbevoegdheid.

Waarborgen voor documentatie, opslag en rechterlijk toezicht

Ten aanzien van het documenteren en loggen van uitvoeringshandelingen geldt dat in vrijwel alle landen een vorm van documentatie vereist is. Dit betekent dat op zijn minst een proces-verbaal moet zijn opgesteld waarin alle handelingen staan gedocumenteerd. Sommige landen gaan een stap verder, omdat daar alle handelingen moeten worden gelogd. Voor vijf landen is gedurende ons onderzoek niet duidelijk geworden of daar eisen worden gesteld aan het documenteren en loggen van uitvoeringshandelingen.

In België, Frankrijk, Kroatië, Portugal en Spanje vindt *gedurende* de inzet van de bevoegdheid rechterlijk toezicht plaats. Dit betekent dat de politie tussentijds aan de rechter die de machtiging heeft verleend statusupdates moet geven over de voortgang. In sommige gevallen kan de rechter op basis daarvan besluiten de toestemming voor de inzet van de bevoegdheid in te trekken. Voor de overige landen geldt dat – voor zover bekend – geen tussentijds rechterlijk toezicht plaatsvindt.

Twintig landen kennen in de wet opgenomen waarborgen ten aanzien van de opslag van gegevens die zijn verkregen met de hackbevoegdheid. Hierbij gaat het onder meer om het verzegeld opslaan van de gegevens of het opslaan van de gegevens in een beveiligde omgeving. Voor de overige landen geldt dat er niets is opgenomen in de wet of dat ons niet duidelijk is geworden of landen (informele) waarborgen kenden.

Notificatieplicht en inzagerecht

In dertien landen is een notificatieplicht opgenomen in de wet. Dat betekent dat personen van wie het geautomatiseerd werk is binnengedrongen binnen een bepaalde termijn geïnformeerd moeten worden dat de bevoegdheid is ingezet. In de helft van

deze landen kan notificatie worden uitgesteld of soms zelfs achterwege blijven als opsporingsbelangen in het gedrang kunnen komen. Voor vrijwel alle landen geldt dat de verdachte wordt genotificeerd, als een zaak ter zitting komt. Verder is in zeventien landen het recht op inzage tot de verkregen gegevens expliciet opgenomen in de wet. In veel gevallen kan de verdediging een kopie van de verkregen gegevens ontvangen. Bij de overige landen is in onze inventarisatie niet naar voren gekomen of voor de bevoegdheid een specifieke wettelijke bepaling is opgenomen ten aanzien van het recht op inzage.

Verdiepende landenvergelijking

In dit onderzoek is ook een aantal landen diepgaander bestudeerd. Deze landen zijn onderling en met Nederland vergeleken. Daarom volgt eerst een beschrijving van de belangrijkste knelpunten in Nederland. Daarna volgt de landenvergelijking.

Belangrijkste (knel-)punten keuring technische hulpmiddelen in Nederland

De Nederlandse wetgever heeft ervoor gekozen om bij de introductie van de hackbevoegdheid het keuringssysteem van technische hulpmiddelen te volgen dat gebruikt wordt voor al bestaande (bijzondere) opsporingsbevoegdheden. Voor de hackbevoegdheid is een apart besluit genaamd 'Besluit onderzoek in een geautomatiseerd werk' (hierna Besluit) ontworpen. In dit Besluit worden diverse eisen gesteld aan een technisch hulpmiddel, waaronder eisen die gericht zijn op de integriteit, herleidbaarheid en betrouwbaarheid (hierna kwaliteit) van de verzamelde gegevens. De Keuringsdienst voert de keuringen in Nederland uit en zij hanteert daarbij een keuringsprotocol dat gebaseerd is op diverse artikelen uit het Besluit. In principe moet de politie gebruik maken van een technisch hulpmiddel dat vooraf (goed-)gekeurd is. Hiervoor geldt een aantal uitzonderingen: 1) een technisch hulpmiddel kan achteraf gekeurd worden; 2) er kan worden overgegaan op een handmatige inzet; of 3) de officier van justitie oordeelt dat het middel 'naar zijn aard' niet te keuren is.

Uit de Verslagen van de Inspectie en het eerste evaluatierapport van het WODC blijkt dat de keuring en het gebruik van technische hulpmiddelen niet altijd verlopen zoals wettelijk bedoeld. Het inzetten van een vooraf goedgekeurd technisch hulpmiddel gebeurt niet of nauwelijks en voor de opsporingspraktijk vormt de keuring een belangrijk knelpunt. Verschillende aspecten spelen hierbij een rol:

- De doorlooptijd van een keuring neemt relatief veel tijd in beslag, tenminste vier maanden. Die tijd past niet altijd bij de snelheid die nodig kan zijn binnen een opsporingsonderzoek.
- Een technisch hulpmiddel aanpassen dat nog niet goedgekeurd is, vereist altijd een nieuwe keuring en kost dus tijd.
- Het Besluit vereist, en daardoor ook de Keuringsdienst, dat een technisch hulpmiddel aan alle eisen dient te voldoen, wil het technisch hulpmiddel goedgekeurd worden. De opsporingspraktijk stelt echter vragen over het nut en de noodzakelijkheid van (het voldoen aan) alle eisen.
- De inzet van technische hulpmiddelen gebeurt in een omgeving die Digit, het politieteam dat de bevoegdheid uitvoert, niet altijd onder controle heeft. Digit heeft bijvoorbeeld géén invloed op wat een verdachte met zijn of haar geautomatiseerd werk doet. Handelingen van de eigenaar van het geautomatiseerd werk kunnen de kwaliteit van de verzamelde gegevens aantasten. Digit zou zich meer willen richten

op het maken van een risicoanalyse met betrekking tot het gebruikte technisch hulpmiddel en op de bewijswaarde van de verzamelde gegevens.
- Bij een risicoanalyse gaat het om de vraag hoe groot het risico is dat de kwaliteit van de gegevens in het gedrang komt als een technisch hulpmiddel wordt gebruikt dat niet aan alle eisen voldoet.
- Het is verder de vraag wat het gebruik van een technisch hulpmiddel, dat niet aan alle eisen voldoet, betekent voor de bewijswaarde van de verzamelde gegevens. Zeker wanneer de gegevens slechts een deel vormen van het bewijs dat verzameld is.

In de opsporingsonderzoeken waarin de hackbevoegdheid in Nederland is ingezet werd in de meerderheid van de onderzoeken gebruik gemaakt van een commercieel product. Ook hiervoor geldt dat geen gebruik is gemaakt van een vooraf goedgekeurd hulpmiddel. Sterker nog, het product is nooit ter keuring aangeboden, omdat de Digit-officier van justitie, de landelijk officier die de bevoegdheid in portefeuille heeft, oordeelde dat de aard van dit hulpmiddel zich verzet tegen een keuring. Daarbij maakte de officier van justitie gebruik van een uitzonderingsgrond in het Besluit. Dit product kan overigens onder het huidige keuringsregime ook niet goedgekeurd worden. Een aantal punten maakt dat dit product naar zijn aard niet te keuren is en/of nooit goedgekeurd zal worden:
- Commerciële middelen worden relatief vaak geüpdatet. De vraag is welke versie(-s) de Keuringsdienst moet keuren. Mocht dit bij alle versies noodzakelijk zijn, dan past dat niet bij de doorlooptijd die een keuring doorgaans in beslag neemt in relatie tot de termijn waarbinnen een inzet plaats moet vinden.
- De exacte werking van dit soort middelen is voor de gebruikers ervan een ‘zwarte doos’. Daardoor krijgt de Keuringsdienst geen inzage in de precieze werking en kan geen volledige keuring plaatsvinden.
- Een leverancier heeft te allen tijde toegang tot zijn product, bijvoorbeeld voor het plegen van onderhoud. Daardoor krijgt de Keuringsdienst geen exclusieve toegang tot het middel, hetgeen voor haar een vereiste is om de keuring te kunnen doen. Geen exclusieve toegang betekent geen goedkeuring, omdat niet uitgesloten kan worden dat een andere partij dan de verdachte en de politie toegang heeft gehad tot de verzamelde gegevens. Dat betekent dat de betrouwbaarheid en de integriteit van de gegevens niet volledig gegarandeerd kunnen worden.

Het niet uitvoeren van een keuring leidt ertoe dat in een meerderheid van de opsporingsonderzoeken niet voldaan wordt aan een belangrijke waarborg ten aanzien van de kwaliteit van de verzamelde gegevens. Daarbij dient opgemerkt te worden dat in deze situatie wel aanvullende technische en tactische waarborgen worden getroffen om de betrouwbaarheid van het bewijs te kunnen garanderen. Deze tactische waarborgen worden tijdens de keuring niet meegenomen.

Landenvergelijking

In ons onderzoek zijn vijf landen meer diepgaand bestudeerd: België, Duitsland, Frankrijk, Zweden en Zwitserland. Om de landen te vergelijken is ten aanzien van de waarborgen onderscheid gemaakt tussen drie fases tijdens de inzet van de hackbevoegdheid: de fase voorafgaand aan de inzet, tijdens de inzet en na de inzet van de hackbevoegdheid.

Waarborgen voorafgaand aan inzet bevoegdheid

Op Zweden na vindt in ieder land een vorm van keuring of toetsing plaats van het te gebruiken technisch hulpmiddel. De wijze waarop verschilt echter per land. Nederland kent de meest gedetailleerde *beschreven* keuring van technische hulpmiddelen. De wijze waarop Duitsland de criteria heeft beschreven lijkt het meest in de buurt te komen bij de wijze waarop Nederland dat heeft gedaan. De Duitse keuring is gebaseerd op de SLB-richtlijn, waarbij de volgende thema's centraal staan: beschermingsdoelen en veiligheidsmaatregelen, werkprocessen en procedures, leveranciers en testbeleid. Het hanteren van de richtlijn is geen wettelijk vereiste, maar geldt als leidraad. Aan de hand van een risicoanalyse wordt voor deze thema's in kaart gebracht welke objecten (denk aan systeemcomponenten zoals hard- en software, applicaties, organisatorische of personele aangelegenheden) risico opleveren. De resultaten van die risicoanalyse, de vaststelling van de beschermingsbehoeften en de daaruit voortvloeiende gevolgen en de uitvoering ervan, worden vastgelegd in een IT-beveiligingsconcept. Zowel leveranciers van software als gebruikers van de software dienen zich aan dit concept te conformeren. In de overige landen is niet bekend welke criteria deel uitmaken van de keuring.

In Nederland wordt de keuring uitgevoerd door de Keuringsdienst. De Keuringsdienst is onafhankelijk, maar valt formeel onder hetzelfde organisatieonderdeel van de Nationale Politie als waar het team toebehoort dat de bevoegdheid uitvoert. In Frankrijk voert een specifieke overheidsinstantie genaamd STNCJ de keuring uit. Deze instantie is ook verantwoordelijk voor de uitvoering van de bevoegdheid. In beide landen kan door de wijze waarop de taken zijn belegd de vraag rijzen hoe onafhankelijk de keuring is. Dit geldt in het bijzonder voor Frankrijk, waarbij het ook daadwerkelijk dezelfde organisatie is die uitvoert en keurt. In de andere landen toetst de politie zelf. Interessant om op te merken is dat in Frankrijk en Zwitserland de 'keurder' en uitvoerder dezelfde partij zijn. In deze landen wordt dit niet als problematisch gezien en wordt aangenomen dat de partijen in principe vertrouwenswaardig handelen. In Zweden vindt – voor zover bekend – geen formele keuring plaats. Wel wordt daar later in het proces van het hacken – als de gegevens op de systemen van de politie staan – veelal gebruik gemaakt van gestandaardiseerde software. Dit is bijvoorbeeld software gecertificeerd door andere politiediensten, zoals de Nederlandse politie.

Waarborgen tijdens inzet bevoegdheid

De waarborgen tijdens de inzet van de bevoegdheid verschillen per land. Gangbare waarborgen in deze fase zijn vormen van logging, verslaglegging, het gebruik van een beveiligd transport van gegevens afkomstig uit het geautomatiseerd werk en het opslaan van de gegevens in een beveiligde omgeving.

In België en Frankrijk vindt gedurende de inzet van de bevoegdheid rechterlijk toezicht plaats. De rechter die toestemming verleent voor de inzet van de bevoegdheid houdt ook toezicht op de uitvoering van de bevoegdheid. Indien de uitvoering van de bevoegdheid niet conform de voorwaarden van de toestemming plaatsvindt, kan de inzet van de bevoegdheid worden stopgezet. Daarbij moet worden opgemerkt dat de rechter afhankelijk is van de informatie die de politie of de officier van justitie tussentijds verstrekt of kan verstrekken. Het is dan ook de vraag of dit rechterlijk toezicht er daadwerkelijk voor zal zorgen dat een inzet tussentijds beëindigd kan worden. Het rechterlijk toezicht in deze landen gaat verder dan de rol van de rechter-

commissaris in Nederland, die in principe alleen voorafgaand aan een inzet (of een verlenging ervan) meekijkt. Wel kent Nederland nog het toezicht door de Inspectie Justitie en Veiligheid.

Waarborgen na inzet bevoegdheid

De meest voorkomende waarborgen hebben betrekking op de notificatie van de inzet van de bevoegdheid aan de verdachte(-n) of betrokkene(-n), de inhoudelijke behandeling tijdens de zitting en het inzagerecht van de verdachte. Notificatie is niet in alle landen gegarandeerd, omdat dit soms achterwege kan blijven indien het risico bestaat dat lopende opsporingsbelangen worden geschaad. In België moet op basis van de wet altijd genotificeerd worden. Frankrijk is het enige land waarin een verdachte niet genotificeerd hoeft te worden. Uiteraard geldt dat indien de gehackte gegevens deel uitmaken van de bewijsvoering de verdachte door inzage in het dossier indirect wordt genotificeerd. Welke informatie in het dossier wordt opgenomen, en tot hoever het inzagerecht strekt, is niet voor alle landen duidelijk geworden. Wel komt naar voren dat in de meeste gevallen de verdediging een kopie ontvangt van (een selectie van) de gegevens die verzameld zijn met de hackbevoegdheid.

Op basis van de interviews blijkt dat nog weinig jurisprudentie beschikbaar is waarin de kwaliteit van de gegevens, verzameld met behulp van de hackbevoegdheid, ter discussie is gesteld. Dat maakt het lastig om de vraag te beantwoorden in welke mate een zittingsrechter de inzet van de bevoegdheid en de kwaliteit van de gegevens toetst. De jurisprudentie die ons wel bekend is gaat veelal over zaken waarin bewijs wordt gebruikt gebaseerd op gegevens van de communicatiedienst Encrochat. De Franse autoriteiten hebben deze communicatie kunnen onderscheppen. In veel landen zijn Encrochat-gegevens gebruikt als bewijs. Bij de behandeling van deze zaken stond echter vooral de vraag centraal of het verkregen bewijs rechtmatig was en niet de vraag wat de kwaliteit van de verzamelde gegevens was. Voor zover bekend is alleen in Zweden en Frankrijk de kwaliteit van gegevens ter discussie gesteld. In Zweden verwierp de rechtbank relatief eenvoudig de geuite bezwaren ten aanzien van de kwaliteit van de gegevens. Opvallender is een arrest van oktober 2022 uit Frankrijk. Daarin concludeert de rechter dat, bij gebrek aan een certificaat van waarheids-getrouwheid, het niet wordt geaccepteerd dat niets gedeeld wordt over de wijze waarop het bewijs verkregen is.. Dit geldt echter alleen als de verzamelde gegevens versleuteld zijn. Het ligt voor de hand dat de politie de bevoegdheid juist inzet om ontsleutelde berichten (live) te kunnen inzien. In deze gevallen is een certificaat dus niet benodigd.

Een ander opvallend punt ten aanzien van de waarborgen na afloop van de inzet is de wettelijke bepaling in Zwitserland dat de broncode van het technisch hulpmiddel gecontroleerd moet kunnen worden als de rechtbank daar om vraagt. Voorafgaand aan de inzet moet ook worden verzekerd dat de leverancier geen toegang kan krijgen tot de gegevens. Het prijsgeven van de broncode en de toegangsbeperking vallen op, omdat beide punten in Nederland een belangrijk obstakel vormen om commerciële middelen (goed) te keuren. Een relevante vraag, die helaas niet beantwoord kan worden op basis van ons onderzoek, is daarom in hoeverre beide vereisten uiteindelijk afgedwongen kunnen worden in Zwitserland.

Ten slotte valt op dat Zweden het enige van de vijf landen is dat een specifieke toezichthouder (SIN) kent die toezicht houdt op de bevoegdheid. De rol van SIN ten aanzien van de inzet van technische hulpmiddelen voor de hackbevoegdheid is nog in

ontwikkeling. Het toezicht richt zich vooralsnog vooral op de juridische en procesmatige aspecten van de bevoegdheid (zoals de rechtmatigheid). SIN heeft echter de bevoegdheid om ook naar de technische hulpmiddelen zelf te kijken.

Scenario's

Op basis van ons onderzoek hebben wij een drietal scenario's geformuleerd die mogelijk een aanvulling kunnen bieden op de wijze waarop in Nederland met technische hulpmiddelen en gegevens, verzameld middels de hackbevoegdheid, wordt omgegaan. Deze scenario's worden in onderstaande tekst beschreven.

Scenario 1: Broncode en controle op toegang gegevens

In ons onderzoek komt naar voren dat het in Zwitserland wettelijk verplicht is dat de broncode van het technisch hulpmiddel gecontroleerd moet kunnen worden als de rechtbank daar om vraagt. Daarnaast moet verzekerd worden dat de leverancier geen toegang kan krijgen tot de gegevens wanneer deze verzameld worden. Juist deze twee punten vormen een belangrijk obstakel in Nederland om commerciële technische hulpmiddelen te keuren. Het is niet duidelijk geworden in hoeverre de Zwitserse autoriteiten daadwerkelijk beide vereisten hebben kunnen realiseren. Voor zover bekend is er nog geen zaak geweest waarin daadwerkelijk om de broncode is gevraagd. De leverancier heeft er in beginsel geen baat bij om inzage te geven in zijn broncode. De werkwijze van de software is een goed bewaard geheim. Echter, als Zwitserland een werkbare oplossing heeft kunnen vinden, is het voor de politie, het Openbaar Ministerie en beleidsmakers in Nederland waardevol om te verkennen hoe dit op een soortgelijke manier gerealiseerd kan worden. Daarmee zouden twee belangrijke knelpunten bij de keuring in Nederland opgeheven kunnen worden.

Scenario 2: Veranderende rol toezicht

Gedurende het Nederlandse wetstraject is het toezicht tijdens de inzet van de bevoegdheid een belangrijk discussiepunt geweest. Extra toezicht zou nodig zijn omdat rechters niet altijd in staat zouden zijn om het verzamelde bewijs goed te beoordelen. Ook was de verwachting dat een (groot) deel van de zaken nooit door een zittingsrechter behandeld zou worden. Er is geopperd om een vergelijkbaar orgaan in het leven te roepen als de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Verschillende auteurs hebben in de loop van de tijd gewezen op het belang van (extra) toezicht, dan wel een andere vorm van toezicht. De wetgever heeft uiteindelijk niet gekozen voor een commissie vergelijkbaar met de CTIVD. Argumenten hiervoor waren het reeds bestaande toezicht door een rechter-commissaris en het toezicht door de Centrale Toetsingscommissie van het Openbaar Ministerie. In plaats daarvan is gekozen voor de Inspectie Justitie en Veiligheid, die toezicht houdt op zaken die wel en niet aan de rechter worden voorgelegd.
Op basis van ons onderzoek nemen wij geen positie in ten aanzien van deze discussie. Wel is het relevant om te noemen dat, als ten aanzien van de hackbevoegdheid de rol van het toezicht verder wordt verkend, een aantal landen uit onderhavig onderzoek mogelijke handvatten kan bieden.

Ten eerste is in dit kader relevant dat in België en Frankrijk een onderzoeksrechter toezicht houdt op de uitvoering van de bevoegdheid. De rechter die toestemming verleent voor de inzet van de bevoegdheid houdt ook toezicht op de uitvoering van de

bevoegdheid. Indien nodig kan de rechter besluiten de inzet van de bevoegdheid stop te zetten. Dit toezicht gaat verder dan de rol van de rechter-commissaris, die in principe alleen voorafgaand aan een inzet controle uitoefent. De werkwijze in België en Frankrijk ondervangt het probleem dat een deel van de zaken niet door de zittings-rechter wordt behandeld. Als kanttekening moet worden opgemerkt dat de rechter afhankelijk is van de informatie die hij of zij verstrekt krijgt. Het is dan ook de vraag of dit rechterlijk toezicht er daadwerkelijk toe leidt dat gedurende een inzet een inhoudelijke toets plaatsvindt. Wel biedt het een perspectief dat afwijkt van de Nederlandse systematiek, waarin de rechter-commissaris voorafgaand toestemming verleent en daarna in principe niet meer toeziet op de uitvoering van de bevoegdheid.

Ten tweede is de Zweedse toezichthouder (SIN) relevant. Deze toezichthouder houdt specifiek toezicht op de uitvoering van de hackbevoegdheid. Hij lijkt daarmee op de mogelijke introductie van een commissie naar voorbeeld van de CTIVD. SIN richt zich vooralsnog primair op de juridische en procesmatige aspecten van de bevoegdheid (zoals de rechtmatigheid) en houdt zowel toezicht op de activiteiten van de politie als van het Openbaar Ministerie. Hiermee onderscheidt hij zich van de taken van de Inspectie in Nederland die alleen toezicht houdt op de politie. Daarnaast kan SIN op verzoek en uit eigen beweging publiekelijk uitspraken doen in individuele zaken. Doordat SIN zich zowel richt op de juridische als op de procesmatige aspecten worden de eerder aangehaalde problemen ondervangen dat niet alle zaken voor een zittingsrechter komen en dat de rechter niet altijd voldoende in staat zou zijn al het bewijs goed te beoordelen.

Scenario 3: Keuring op maat

Zoals reeds besproken vormt de keuring in Nederland een belangrijke waarborg bij de inzet van technische hulpmiddelen en de kwaliteit van de gegevens die met het middel worden verzameld. In de praktijk blijkt dat de keuring en het gebruik van technische hulpmiddelen niet altijd verlopen zoals wettelijk is bedoeld. Er wordt voornamelijk gebruik gemaakt van niet vooraf goedgekeurde technische hulpmiddelen en technische hulpmiddelen die naar hun aard niet te keuren zijn. Opvallend is dat in het buitenland de waarborgen rondom technische hulpmiddelen en de kwaliteit van gegevens wettelijk minder gedetailleerd beschreven zijn dan in Nederland. In dat opzicht is het in het buitenland gemakkelijker om de bevoegdheid in te zetten. Ook valt op dat in die landen (vooralsnog en voor zover ons bekend) niet of nauwelijks jurisprudentie beschikbaar is die het gebruik van de hackbevoegdheid in deze landen ter discussie stelt. Dat betekent overigens niet dat het bewijs van de hackbevoegdheid altijd zomaar geaccepteerd zal worden. In veel landen is de hackbevoegdheid relatief nieuw en zal het gebruik ervan en een oordeel daarover zich nog verder ontwikkelen. Het valt dan ook niet uit te sluiten dat in de toekomst alsnog uitspraken volgen die gevolgen hebben voor het huidig wettelijke kader in deze landen. Dat neemt niet weg dat het interessant is om te constateren dat in de verschillende landen niet de keuze is gemaakt om de kwaliteit van de gegevens te controleren op een wijze waarop Nederland dat doet. En dat de buitenlandse manier van werken voor zover bekend vooralsnog niet tot wezenlijke discussies in de rechtbank heeft geleid. Daarom hebben we een derde scenario opgenomen waarin oog is voor meer maatwerk ten aanzien van de keuringseisen, waarbij aandacht is voor aanvullende tactische en technische waarborgen. Dit scenario verkent a) het gebruik van een risicoanalyse in de keuring en b) de vraag in hoeverre aanvullende tactische en technische maatregelen voldoende gewaarborgd zijn.

Scenario 3a: Risicoanalyse in de keuring

In Duitsland speelt het maken van risicoanalyses een rol wanneer het gaat om de aanschaf en het gebruik van technische hulpmiddelen. In een SLB-richtlijn worden diverse onderwerpen genoemd waarmee rekening zou moeten worden gehouden als het gaat om technische hulpmiddelen, zoals het testbeleid. Aan de hand van een risicoanalyse wordt voor deze thema's in kaart gebracht welke objecten risico lopen en welke aanvullende maatregelen nodig zijn. De verschillende betrokken partijen dienen zich hieraan te conformeren. In Nederland geeft de uitvoerende partij (Digit) aan dat de Keuringsdienst (en het onderliggende keuringsprotocol) onvoldoende rekening houdt met het feit dat zij ook zou kunnen werken op basis van risicoanalyses, namelijk wat betreft de maatregelen die zij neemt wanneer zij een inzet doet met een technisch hulpmiddel. Juist deze risicoanalyse lijkt een meer centrale plek te hebben in Duitsland. Daarom zou de werkwijze in Duitsland nader verkend kunnen worden om te zien wat daaruit geleerd kan worden voor de Nederlandse situatie.

Scenario 3b: Borging aanvullende tactische waarborgen in Nederland

Zoals opgemerkt, wordt in Nederland op dit moment primair gebruikgemaakt van technische hulpmiddelen waarvan de officier van justitie oordeelt dat ze naar hun aard niet te keuren zijn. In deze situatie worden tactische en technische maatregelen getroffen om de kwaliteit van de gegevens te waarborgen. Voor nu zijn er geen aanwijzingen dat het gebruik van commerciële producten beëindigd zal worden. De huidige minister ziet deze als 'een realiteit waar we mee te dealen hebben', zo blijkt uit een Commissiedebat op 7 juli 2022. Het gebruik van risicoanalyses beschreven in scenario 3a kan een handvat bieden om juiste aanvullende maatregelen te treffen om de kwaliteit van de gegevens te waarborgen. Indien de werkwijze met commerciële producten eerder regel dan uitzondering blijft en exact op dezelfde manier gewerkt zal blijven worden, is het ook van belang de rol van het Openbaar Ministerie ten aanzien van de aanvullende (tactische) waarborgen tegen het licht te houden. Op dit moment is het de enige die voorafgaand aan een inzet de tactische waarborgen bekijkt. Een tactisch officier van justitie die het opsporingsonderzoek leidt is in principe eindverantwoordelijk voor deze waarborgen. Deze worden ook bekeken door de Digit officier van justitie en de Centrale toetsingscommissie van het Openbaar Ministerie. Vanwege enkel de betrokkenheid van het Openbaar Ministerie en geen andere onafhankelijke instantie, is het nuttig om te verkennen welke andere partij (aanvullend) kan controleren of deze maatregelen toereikend zijn, zeker in gevallen dat een zittingsrechter een zaak niet zal behandelen.

References

General

Boeije, H. (2007). *Analyseren in kwalitatief onderzoek: Denken en doen*. Boom Onderwijs.

Berndsen, M. (2022, 17 september 2022). Twitter. www.twitter.com/cyberadvocaat/status/1571149854180782081.

Buruma, Y. (2016). *De criminele homo digitalis,* NJB 2016/1073, afl. 22, 1534-1541.

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving*.

Corstens, G. J. M., Borgers, M. J., & Kooijmans, T. (2018). *Het Nederlands strafprocesrech*t. (9de dr.). Wolters Kluwer.

Det Kongelige Justig- og Beredskapsdepartement (2016). *Prop. 68 L (2015–2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler).* Accessed 24 April 2023:: www.regjeringen.no/no/dokumenter/prop.-68-l-20152016/id2479232/.

Det Uafhængige Tilsyn med Bevismidler (z.d.). *Velkommen til Det Uafhængige Tilsyn med Bevismidler*. Accessed 24 April 2023: www.bevismiddeltilsynet.dk/.

Eurojust (2016). *Cybercrime Judicial Monitor*. Accessed 29 March 2023: www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016-11_CJM-2_EN.pdf.

Eurojust (z.d.). *European Judicial Cybercrime Network*. Accessed 29 March 2023: www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network.

Eurojust (z.d.). *Mission*. Accessed 29 March 2023: www.eurojust.europa.eu/about-us/organisation/mission.

Fedorova, M. I., Te Molder, R. M., Dubelaar, M. J., Lestrade, S. M. A., & Walree, T. F. (2022). *Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunten bij de normering van het werken van persoonsgegevens voor strafvorderlijke doeleinden*. Radboud University Press.

Gutheil, M., Liger, Q., Heetman, A., Eager, J., & Crawford, M. (2017). *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Policy Department for Citizens' Rights and Constitutional Affairs. Accessed 29 March 2023: www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

Hildebrandt, M. (2016). Data-gestuurde intelligentie in het strafrecht. In E. M. L. Moerel, J. E. J. Prins, M. Hildebrandt., T. F. E, Tjong Tjin Tai, G. J. Zwenne & A. H. J. Schmidt. (Red.), *Homo Digitalis, Handelingen 146e NJV vergadering 2016* (pp. 137-240). Kluwer.

Hirsch Ballin, M. F. H. & Oerlemans, J-J. (2023). Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden. *Delikt en Delinkwent*, *1*(2), 18-38.

Home Office (2018). *Equipment interference: Code of practice*. Accessed 24 April 2023: www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International, 2*, 1-6.

Inspectie JenV (Justitie en Veiligheid) (2020). *Verslag toezicht wettelijke hack-bevoegdheid politie 2019: Verslag van het toezicht door de Inspectie Justitie en Veiligheid op de toepassing door de politie van de bevoegdheid op basis van de wet*

Computercriminaliteit III om in een geautomatiseerd werk binnen te dringen en onderzoek te doen. Inspectie Justitie en Veiligheid. www.inspectie-jenv.nl/Publicaties/rapporten/2020/08/20/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019.
Inspectie JenV (Justitie en Veiligheid) (2021). *Verslag toezicht wettelijke hackbevoegdheid politie 2020: Heeft de politie zich aan de regels gehouden bij het toepassen van de bevoegdheid tot binnendringen in een geautomatiseerd werk?* Inspectie Justitie en Veiligheid. www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020.
Inspectie JenV (Justitie en Veiligheid) (2022). *Verslag toezicht wettelijke hackbevoegdheid politie 2021: Toezicht op de toepassing door de politie van de bevoegdheid tot het binnendringen en doen van onderzoek in een geautomatiseerd werk*. Inspectie Justitie en Veiligheid. www.inspectie-jenv.nl/Publicaties/rapporten/2022/05/31/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2021.
Ministerio Fiscal (2019). *Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre sobre registro de dispositivos y equipos informáticos*. Accessed 24 April 2023: www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244.
Mayer, J. (2018). Government hacking. *The Yale Law Journal,* 570-662.
Oerlemans, J-J. (2018). *Beschouwing rapport Commissie-Koops: Strafvordering in het digitale tijdperk*. Platform Modernisering Strafvordering november 2018. DOI: 10.5553/PMSV/258950952018001018001.
Jurić, M., & Roksandić, S. (2021). Croatia. In: Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis. *Duncker & Humblot,* 373-419.
Schermer, B. W. (2017). *Software Agents, Surveillance, and the Right to Privacy: A Legislative Framework for Agent-enabled Surveillance.* Leiden University Press.
Sommer, P. (2022). Evidence from hacking: A few tiresome problems. *Forensic Science International, 40*, 1-7.
Van Uden, A., & Van den Eeden, C. A. J. (2022). *De hackbevoegdheid in de praktijk: Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv)*. WODC. Cahier 2022-8. www.repository.wodc.nl/handle/20.500.12832/3202.
Verdelho, P. (2021). Portugal. In U. Sieber & N. von zur Muhlen (Red.), *Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis* (pp. 1221-1281). Duncker & Humblot. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Reihe S: Strafrechtliche Forschungsberichte (MPIS), Volume 156.
Verrest, P. A. M., & Mevis, P. A. M. (2018). *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering*. Boom Juridisch.

Belgium

Belgisch Staatsblad (2018, 19 november). *Publicatie overeenkomstig artikelen 472 tot 478 van de programmawet van 24 december 2002, gewijzigd door de artikelen 4 tot en met 8 van de wet houdende diverse bepalingen van 20 juli 2005*.
Comité P (z.d.). *Ons mission statement*. Accessed 14 December 2022: www.comitep.be/mission-statement.html.
Conings, C. (2020, 26 februari). Grondwettelijk hof en Cassatie op één lijn: Bevel aan verdachte tot overhandiging van digitale toegangssleutel is wettig. *De Juristenkrant.*
Etsi (2020). *Etsi, the essentials*. Accessed 29 March 2023: www.etsi.org/images/files/Brochures/ETSI-essentials.pdf.

Etsi (z.d.). *Etsi in Europe*. Accessed 29 March 2023: www.etsi.org/about/etsi-in-europe.
Etsi (z.d.). *Standards*. Accessed 29 March 2023: www.etsi.org/standards#page=1&search=lawful%2Binterception&title=1&etsiNumber=1&content=0&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2023-03-28&harmonized=0&keyword=&TB=386,,180&stdType=&frequency=&mandate=&collection=&sort=1.
Jobpol.be (z.d.). *Jobs als burger (CALog).* Accessed 31 May 2023: https://www.jobpol.be/nl/jobs-als-burger-calog
Kerkhofs, J., & Van Linthout, P. H. (2019). *Cybercrime 3.0.* Politeia.
Memorie van toelichting bij wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties. 8 juli 2016. Parl*. St.* Kamer 2015-16, nr. 54 1966/001. Accessed 17 November 2022: www.dekamer.be/FLWB/PDF/54/1966/54K1966001.pdf.
Ministère public (z.d.). *Over ons*. Accessed 14 December 2022: www.om-mp.be/fr/uw-om/parketten-arbeidsauditoraten-generaal/gent/parketten/over-ons.
Royer, S., & Yperman, W. (2020). Bewijsverzameling in digitale omgeving door politieambtenaren. In C. De Poot, E. Lievens, W. Stol & L. De Kimpe. (Red.), *Politie en Cybercrime*. Gompel & Svanica. *Cahier Politiestudies,* 2020/3, 23-37.
Strafwetboek België. Accessed 20 December 2022: www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=1867060801.
Traest, P. H. (2019). België. In: P. A. M. Verrest, & P. A. M. Mevis. (2018). *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering*. Boom Juridisch. 19-80.
Yperman, W., Royer, S., & Verbruggen, F. (2019). Vissen op de grote datazee: Digitale informatievergaring in vooronderzoek en strafuitvoering. *Nullum Crimen: Tijdschrift voor Straf- en Strafprocesrecht 2019*(5). 389-416.
Wetboek van Strafvordering België. Accessed 20 December 2022: www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=nl&nm=1808111701&la=N.

Germany

BKA (z.d.). *Quellen-TKÜ und Online-Durchsuchung*. Accessed 12 January 2023: www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.
BKA (2018). *Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online Durchsuchung (Stand 05. Oktober 2018).* Accessed 12 January 2023: www.polizei.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.html.
Bundesamt für Justiz (z.d.). *Statistiken der Rechtspflege*. Accessed 3 January 2023: www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152.
Bundesministerium des Innern (2017). *Erlass über die Errichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich. Vom 6. April 2017*. Accessed 31 March 2023: www.zitis.bund.de/DE/WerWirSind/_documents/ministerialerlass_ZITiS.pdf?__blob=publicationFile&v=3.

Bundesministerium der Justiz (z.d.). *Aktuelle Gesetzgebungsverfahren*. Accessed 31 March 2023: www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Gesetz_zur_effektiveren_und_praxistauglicheren_Ausgestaltung_des_Strafverfahrens.html.
Bundesverfassungsgericht (z.d). *Headnotes to the Judgment of the First Senate of 27 February 2008*. Accessed 31 March 2023: www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.
Deutscher Bundestags (2017). *Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (Drucksache 18/12785).* Accessed 25 January 2023: www.dserver.bundestag.de/btd/18/127/1812785.pdf.
Fedorova, M. I., Te Molder, R. M., Dubelaar, M. J., Lestrade, S. M. A., & Walree, T. F. (2022). *Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunten bij de normering van het werken van persoonsgegevens voor strafvorderlijke doeleinden*. Radboud University Press.
Flade, F. (2018, 2 februari). *Ministerium gibt neuen Bundestrojaner für den Einsatz frei*. Welt. Accessed 21 April 2023: www.welt.de/politik/deutschland/article173121473/Verdeckte-Ueberwachung-ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html.
Groothuis, M. (2008). Bundesverfassungsgericht stelt grenzen aan online doorzoeken van personal computers. *NCJM-Bulletin, 33*(7), 990-1004.
Klip, A., Peristeridou, C. & De Vocht, D. (2019). *Citius, altius, fortius - Sneller, hoger, sterker: Wat we van Engeland en Duitsland kunnen leren in het kader van modernisering Strafvordering*. Maastricht University.
Lindemann, M. & Van Toor, D. (2018). Protection of a suspect's privacy in criminal procedures. *Ars Aequi, 67*(5), 376-384.
Meister, A. (2018, 26 juni). *Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen*. Netzpolitik.org. Accessed 21 April 2023: www.netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/.
Niedernhuber, T. (2018). Die StPO-Reform 2017 – wichtige Änderungen im Überblick. *Juristische Arbeitsblätter, 50*(3), 169-175.
Singelnstein, T., & Derin, B. (2017). Das Gesetz zur effektiveren undpraxistauglicheren Ausgestaltung des Strafverfahrens: Was aus der stPO Reform geworden ist. *Neue Juristische Wochenschrift, 70*(37), 2646-2652.
Škorvánek, I., Koops, B-J., Newell, B. C. & Roberts, A. (2020). 'My computer is my castle': New privacy frameworks to regulate police hacking. *BYU Law Review, 2019*(4), 997-1082.
Soiné, M. (2018). Die strafprozessuale Online-Durchsuchung. *Neue Zeitschrift FürStrafrecht, 38,* 497-504.
Struijk, S. (2018). De betrokkenheid van de rechter bij de tenuitvoerlegging van straffen. In P. A. M. Verrest, & P. A. M. Mevis (Reds.), *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering* (pp. 487-538). Boom Juridisch.
Techopeda. (2016). *Software Library*. Accessed 31 March 2023: www.techopedia.com/definition/3828/software-library.
Zitis (z.d.). *Who we are: What else*. Accessed 31 March 2023: www.zitis.bund.de/EN/Home/home_node.html.

France

Goodwin, B. (2022). *French Supreme Court rejects EncroChat verdict after lawyers question secrecy over hacking operation*. Accessed 17 April 2023:

www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy.
Mattatia, F. (2015). Faut-il dépénaliser les hackers blancs? *Revue de science criminelle et de droit pénal comparé*, 4, 837-846.
Ministère de la Justice - Direction des affaires criminelles et des grâces (2019). *Fiche criminologique, juridique ou technique: Captation de données informatiques.*
Verrest, P. A. M. (2018). Frankrijk. In: P.A.M Verrest & P.A.M Mevis. (2018). *Rechtsvergelijkende inzichten voor de modernisering van het Wetboek van Strafvordering* (pp. 19-80). Boom Juridisch.

Sweden

Cameron, I. (2021). Sweden. In U. Sieber, U. & N. von Zur Mühlen, N*. (Red.), Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis* (pp. 1343-1378). Duncker & Humblot.
Klamberg, M. (2020). *Evidentiary Matters in the Context of Investigating and Prosecuting International Crimes in Sweden: Admissibility, Digital Evidence and Judicial Notice*. Faculty of Law, Scandinavian Studies in Law. Stockholm University Research Paper No. 85
Wong, C. (2012*). Overview of Swedish Criminal Procedure*. Accessed 11 June 2023: www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_10/spl_85/pdfs/24.pdf

Switzerland

Bundesgerichtsentscheid (BGE). *Urteilskopf. 138 IV 232*. Accessed 4 May 2023: www.relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F138-IV-232%3Ade&lang=de&type=show_document.
Basanisi, M. (2019). GovWare – Legiferierung und grundrechtliche Herausforderungen Geheime Überwachung verschlüsselter Kommunikation im Kontext der neuen Schweizer Gesetzgebung zum Einsatz besonderer Informatikprogramme nach Art. 269ter und Art. 269quater StPO. *Jusletter* 14 janvier 2019.
Betschman, S., & Murer Mikolásek, A. (2018). Anwendungsmöglichkeiten von GovWare. *AJP/PJA 6/2018*, 748-752. Accessed 17 April 2023: www.betschmann.ch/AJP_Anwendungsm%C3%B6glichkeiten_von_GovWare.pdf.
Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Accessed 17 April 2023: www.fedlex.admin.ch/eli/cc/2018/31/de.
Eidgenössische Justiz- und Polizeidepartement (EJPD) (2019, 27 februari). *Besondere Informatikprogramme: die Kosten werden geteilt*. Accessed 29 March 2023: www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2019/2019-02-27.html.
Eidgenössische Justiz- und Polizeidepartement (EJPD) (2019b). *Erläuterungen zur Revision der Verordnung über Gebühren für Verfügungen und Dienstleistungen des Bundesamtes für Polizei (Gebührenverordnung fedpol, GebV-fedpol)*. Accessed 29 March 2023: www.digitale-gesellschaft.ch/uploads/2020/01/erl-vo-d.pdf.
Eidgenössische Justiz- und Polizeidepartement (EJPD) (2022). *Statistik*. Accessed 29 March 2023: www.li.admin.ch/de/stats.
Eidgenössische Justiz- und Polizeidepartement (EJPD) (2023). *Häufig gestellte Fragen FAQ - Bundestrojaner/GovWare*. Accessed 29 March 2023: www.li.admin.ch/de/dokumentation/faq.

Engler, S. (2015). Speech Engler Stefan. In: *Amtliches Bulletin – Ständerat. Wintersession 2015. Fünfte Sitzung. 07.12.15. 15h15. 13.025.* Accessed 3 May 2023: www.parlament.ch/en/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-videos?TranscriptId=192170.

Fedlex (2017, 11 januari). *Verordnung über Gebühren für Verfügungen und Dienstleistungen des Bundesamtes für Polizei (Gebührenverordnung fedpol, GebV-fedpol).* Accessed 23 March 2023: www.fedlex.admin.ch/eli/oc/2017/60/de.

Godenzi, G. & Caprara, T. (2018). Zwitserland. In P.A.M. Verrest & P.A.M. Mevis (Red.), *Rechtsvergelijkende inzichten voor de moderinisering van het Wetboek van Strafvordering* (pp. 281-332). Boom Juridisch.

Hansjakob, T. (2011). Einsatz von GovWare – zulässig oder nicht? *Jusletter* 5.12.2011, N 16, 30. Accessed 29 March 2023: www.hansjakob.ch/thomas/jusletter_einsatz_govware.pdf.

ProDemos (2022, februari). *Zwitserland*. Accessed 29 March 2023: www.prodemos.nl/app/uploads/2023/01/webdossier-Kiesstelsel-Zwitserland-versie-oktober-2022.pdf.

Schweizerisches Strafgesetzbuch. Accessed 29 March 2023: www.fedlex.admin.ch/eli/cc/54/757_781_799/de.

Verordnung des EJPD vom 15. November 2017 über das beratende Organ im Bereich der Überwachung des Post- und Fernmeldeverkehrs (VBO-ÜPF). Accessed 17 April 2023: www.fedlex.admin.ch/eli/cc/2018/33/de.

Verordnung des EJPD vom 15. November 2017 über die Durchführung der Überwachung des Post- und Fernmeldeverkehrs (VD-ÜPF). Accessed 17 April 2023: www.fedlex.admin.ch/eli/cc/2018/35/de.

Verordnung vom 15. November 2017 über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VVS-ÜPF). Accessed 17 April 2023: www.fedlex.admin.ch/eli/cc/2018/36/de.

Verordnung vom 15. November 2017 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF). Accessed 17 April 2023: www.fedlex.admin.ch/eli/cc/2018/34/de.

Verordnung vom 15. November 2017 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF). Accessed 17 April 2023: www.fedlex.admin.ch/eli/cc/2018/32/de.

Appendix 1 Source overview

Table B1.1 Consulted sources per country

Countries	Interviews					Lit-era-ture	Regu-lation	Euro-just
	Public ministry	Police	Ministry	Science	Overig			
Australia				X		X	X	
Belgium	X		X	X		X	X	
Bulgary								X
Canada				X		X	X	
Germany		X		X	X	X	X	X
Denmark			X*	X		X	X	
Estonia	X*						X	
Finland					X		X	
France		X*	X			X	X	X
Greece					X		X	
Hungary	X*					X	X	
Ireland				X		X	X	
Italy				X			X	X
Croatia	X*		X*	X		X	X	
Latvia								X
Lithuania	X			X			X	X
Luxembourg	X						X	
Norway		X					X	X
Austria						X		X
Poland				X			X	
Portugal	X*			X		X	X	X
Romania	X						X	
Slovenia				X				X
Slovakia				X*			X	X
Spain				X		X	X	X
Czech Republic	X*			X			X	
United Kingdom				X		X	X	X
United States				X		X	X	
Sweden	X	X	X		X*		X	
Switzerland	X	X	X*			X	X	X

* Concerns an e-mail questionnaire.

Appendix 2 Country overview police hacking

Table B2.1 Country overview police hacking

Country	Provision hacking power	Direct/indirect powers	Type of offence	Investigative activities	Case law
Australia	Division 5 & 6 Surveillance Devices Act (SDA). Division 2 Crimes Act 1914 (Cth).	Direct	Offences punishable by imprisonment for two years or more and 1) is a commonwealth criminal offence, 2) is a crime against the state, 3) is a crime against a law of a territory and does not qualify as a serious terrorist offence (Part IAA, Division 1, 3C Interpretation, Cth).	Disrupting data to prevent or stop criminal acts (such as taking child pornography offline) (Division 5 SDA), monitoring network activities to gain an understanding of criminal networks (Division 6 SDA) and finally taking over an account (Part IAAC,Division 2 Cth).	Not as far as is known.
Belgium	Sections 89ter and 90ter Code of Criminal Procedure (CCP).	Direct	Long list of offences enumerated in Section 90ter (2) CCP, including: assault on the life or person of the king (s. 101 PC), recording non-public communications without permission (s. 314bis PC) and manslaughter to facilitate extortion or theft (s. 475 PC).	Section 89ter CCP: Searching computer systems. No data may be recorded, except a 'sample' for illustrative purposes (similar to taking a sample of drugs during a search). Section 90ter CCP: No restrictions as to the type of data and searching and recording this data, which means that most investigative activities can be carried out, such as interception of communications, turning on a microphone or camera (surveillance) and requesting the location.	Not as far as is known.
Bulgaria	No statutory powers.	N/A	N/A	N/A	N/A
Canada	Section 487.01 of the Criminal Code (CC).	Indirect	No restrictions as to the type of offences under Section 487.01(1)(a) CC. It is for the court to decide whether the tool may be used.	No explicit statements on investigative activities that are permitted. The court's permission is required for any investigative activities to be carried out. This may include both stored and streaming data.	Not as far as is known.

Country	Provision hacking power	Direct/indirect powers	Type of offence	Investigative activities	Case law
Denmark	Sections 791b and 799 Administration of Justice Act (AJA).	Direct	Section 791b AJA: offences punishable by imprisonment for six years or more or violating Chapter 12 or 13 of the Criminal Code, such as terrorism or offences against the Constitution. Section 799 AJA: long list of offences mentioned in paragraph 1. Including: offences against state autonomy and security, serious drug-related offences and child pornography.	Section 791b AJA: data reading. Section 799 AJA: secret search. No specific activities described in the Act.	The Supreme Court ruled that the police's intervention in the suspect's Facebook and Messenger profiles using the suspect's passwords could be done according to the rules on repeated secret searches (Weekly Judicial Journal, U 2012.2614 H).
Germany	Sections 100a and 100b Code of Criminal Procedure (CCP).	Direct	Section 100a CCP: long list of offences mentioned in paragraph 2. Covers 'serious' offences such as extortion, drug-related offences and money laundering. Section 100b CCP: long list of offences mentioned in paragraph 2. Covers 'very serious' offences and preparatory activities such as organised crime, aggravated murder and human trafficking.	Section 100a CCP: interception of telecommunication at the source. Section 100b CCP: searching and recording of all data on computer systems (online search).	Federal Constitutional Court decision of 2008: includes for instance the split between Sections 100a and 100b CCP (Bundesverfassungsgericht, n.d).
Estonia	Section 126-1 Code of Criminal Procedure (CCP).	Indirect	Long list of offences mentioned in Section 126-2 CCP. Including murder, deprivation of liberty and money laundering.	In principle, no restrictions as to type of activities, depends on court authorisation.	Not as far as is known.
Finland	Chapter 10, Section 23 Coercive Measures Act (CMA) (*Pakkokeinolaki*).	Direct	Based on Chapter 10, Section 16 CMA, these concern offences punishable by imprisonment for at least four years, drug offences, preparatory activities of terrorism, aggravated customs offence, preparatory activities of hostage-taking and preparatory activities for violent robbery.	Searching and recording of data and interception of communications.	Not as far as is known.
France	Sections 706-95-11 to 706-102-5 and Section D 15-1-6 Code of Criminal Procedure (CCP).	Direct	Terrorism, organised crime (s. 706-73 CCP) and serious economic crime (s. 706-73-1 CCP).	Both stored and streaming data may be recorded (s. 706-102-01 CCP). Examples include text, images and audio (Fiche, July 2019, p. 1-2).	Constitutional review (Le conseil constitutionnel, décision du 8 avril 2022) & Encrochat (ao Le cour de cassation, 11 October 2022)

Country	Provision hacking power	Direct/indirect powers	Type of offence	Investigative activities	Case law
Greece	No statutory powers.	N/A	N/A	N/A	N/A
Hungary	Section 232(1) Code of Criminal Procedure (CCP). The police do not have the power to do this themselves. The Special Service for National Security (SSNS) carries out this task at the request of organisations operating in the criminal justice system, such as the police or the Public Prosecutor's Office.	Direct	Long list of offences mentioned in Section 234 CCP. Including offences for which a prison sentence of five years or more can be imposed or specific offences listed in paragraphs 2 and 3, such as sexual abuse, corruption and insider trading. May also be used if preparatory activities are involved (see paragraph 4).	Gaining access to and storing data from computer systems (covert surveillance) (s. 232(1) CCP). Interception of communications (s. 232(5) CCP).	Not as far as is known.
Ireland	Some observers believe the state may be using the Criminal Justice (Surveillance) Act 2009 to authorise hacking. If the 2009 Act is being used in this way the following conditions would apply.	Indirect	Based on Section 2 Penal Code, these concern offences (including any preparatory acts) for which a prison term of five years or more can be imposed.	No specific activities described in the Act. However, the 2009 Act would not permit interception of telecommunications, text messages and email within the meaning of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.	Not as far as is known.
Italy	Sections 266 and 267 Code of Criminal Procedure (CCP).	Direct	Long list of offences mentioned in Section 266 CCP. Including offences punishable by imprisonment for five years or more, drug offences, smuggling and arms offences.	Interception of communications on a portable electronic device. A microphone may also be switched on at specific times on a portable electronic device (surveillance).	A lot of case law is available before the powers were introduced in 2017. The arrival of the powers has made this case law obsolete. Since the introduction of the new powers, there has been one judgment confirming that the use of the current powers is lawful (personal communication, 12 may 2022).
Croatia	Section 332 Code of Criminal Procedure (CCP).	Indirect	Long list of offences mentioned in Section 334 CCP. Including offences punishable by imprisonment for five years or more, such as terrorism, child abuse and money laundering.	Monitoring and technical recording of telephone conversations and other means enabling remote technical communication (s. 332(1)(1) CCP). Intercepting, collecting and recording computer data (s. 332(1)(2) CCP). Gaining access to a site so surveillance and technical recordings of the site can take place there (s. 332(1)(3) CCP). Covertly following individuals and objects and making technical	Not as far as is known.

Country	Provision hacking power	Direct/indirect powers	Type of offence	Investigative activities	Case law
				recordings of these (s. 332(1)(4) CCP).	
Latvia	No statutory powers.	N/A	N/A	N/A	N/A
Lithuania	Section 158 Code of Criminal Procedure (CCP) and Section 10 Criminal Intelligence Act (Act).	Indirect	Section 158 CCP: offences punishable by imprisonment of more than three years. Section 10 Act: offences punishable by imprisonment of more thans six years, **many enumerated offences punishable by imprisonment of more than three years,** fugitives, missing persons, security of persons, preventing activities of criminal organisations.	Section 158 CCP: no explicit statements on investigative activities. The order must include the actions that may be taken (s. 158(3) CCP). Sections 2(22), 8, 10 Act: no explicit statements on investigative activities.	Not as far as is known.
Luxembourg	Section 88-1(3) Code of Criminal Procedure (CCP).	Direct	Under Section 88-2(1) CCP, the powers are limited to offences against the state, terrorism and terrorist financing.	It is only possible to wiretap live input and output from a user as displayed on the screen (s. 88-1 CCP).	Not as far as is known.
Norway	Section 216o in conjunction with Section 216p Code of Criminal Procedure (CCP).	Direct	Enumeration of offences in Section 216o(1) CCP. Including offences punishable by imprisonment of ten years or more (under a) and offences listed under b, such as publication of state secrets, participating in a terrorist organisation and human trafficking.	The recording of non-publicly available data in a computer system, including communications, electronically stored data and other information about the use of a computer system or user account (s. 216o(1) and (4) CCP). Involves for instance the following acts: recording audio by using a microphone, recording audio on computer systems, recording video by using a camera, keylogging, obtaining information regarding stored data, interception of internet data and metadata (Det Kongelige Justig- og Beredskapsdepartement, 2016 (Bill)).	Not as far as is known.
Austria	No statutory powers.	N/A	N/A	N/A	N/A
Poland	Section 19(6)(4) Police Act (PA).	Direct	Long list of offences enumerated in Section 19(1) PA. Including murder and manslaughter, human trafficking and child pornography.	Section 19(6) PA describes the acts that may be carried out covertly: interception of communications, turning on microphones and cameras in specific rooms (surveillance), searching and recording stored	Not as far as is known.

Country	Provision hacking power	Direct/indirect powers	Type of offence	Investigative activities	Case law
				communications, searching and recording data from computer systems and accessing and searching an email box.	
Portugal	Section 19 Cybercrime Act, Section 187 Code of Criminal Procedure (CCP) in conjunction with Sections 188 and 189 and Act No. 05/2002. These articles are leading, but their scope is questioned by some authors (personal communication, 15 June 2023).	Indirect	Section 19 Cybercrime Act: list of offences laid down in the Cybercrime Act and other forms of crime committed using a computer system and punishable by imprisonment for at least five years. In addition, a number of other offences are mentioned regardless of their punishment, including offences impeding sexual freedom and self-determination when committed against minors and persons with disabilities, aggravated fraud and other economic and financial offences, racial, religious and sexual discrimination and offences related to infringements of copyright and related rights. Section 187 CCP: list of various offences, including offences punishable by imprisonment for at least three years or more, drug-related offences, kidnapping and hostage-taking and offences against state security. Act 05/2002: various offences laid down in Section 1(1-4). Including drug trafficking, terrorism, corruption, arms trafficking, money laundering and child pornography (s. 1(1) Act 05/2002).	Section 19 Cybercrime Act: activities that can be carried out under Section 19 of the Cybercrime Act are not explicitly stated in the Act (Verdelho, 2021, pp. 1260-1261). Section 187 CCP: Interception and recording of telephone calls and communications (s. 187(1) CCP). Act 05/2002: Registering of sound and images (s. 6 Act No. 05/2002).	Not as far as is known.
Romania	Sections 138 and 139 Code of Criminal Procedure (CCP).	Direct	Section 139(2) CCP mentions the following offences: offences punishable by imprisonment of five years or more. In addition, the following specific offences: drug trafficking, offences against national security, human trafficking, terrorism, money laundering, forgery of money and securities, forgery	Section 138 CCP describes the following acts: a) interception of communications; b) gaining access to computer systems; c) turning on a microphone or camera (surveillance); d) location tracking and e) obtaining information on financial transactions of individuals.	Not as far as is known.

Country	Provision hacking power	Direct/indirect powers	Type of offence	Investigative activities	Case law
			of electronic payment instruments, property offences, extortion, rape, deprivation of liberty, tax evasion, corruption, offences against the financial interests of the European Union and computer crime.		
Slovenia	No statutory powers.	N/A	N/A	N/A	N/A
Slovakia	Section 115 Code of Criminal Procedure (CCP).	Direct	Section 115 CCP (1) lists the following offences: corruption, criminal offences of extremism, a criminal offence of abuse of authority of a public official, a criminal offence of money-laundering offence described in Sections 233 and 234 PC or another intentional criminal offence, the performance of which is bound by an international treaty.	Interception of all forms of communication (image, sound and data) (personal communication, 8 August 2022).	Not as far as is known.
Spain	Section 588 et seq. Code of Criminal Procedure (CCP).	Direct	List of offences mentioned in Section 588(1) CCP. Offences committed by criminal organisations, terrorism, offences committed against minors or legally incapacitated persons, offences against the Constitution, treason and offences related to national defence and computer crime.	Online examination. No specific activities described in the law. See Section 588(1) CCP.	Not as far as is known.
Czech Republic	Section 158d(3) Code of Criminal Procedure (CCP).	Indirect	No restriction on type of offences included in legislation, except that they must be offences committed intentionally (personal communication, 14 June 2023).	No specific activities described in legislation. Anything that takes place on computer systems can be monitored (s. 158d(2) CCP).	Not as far as is known.
United Kingdom	Chapter 5 Investigatory Powers Act (IPA)	Direct	Serious offences (see s. 106 IPA). Covers offences punishable by imprisonment for three years or more or conduct involving the use of violence, conduct resulting in substantial financial gain or conduct carried out by a large number of persons for a common purpose (s. 263 IPA).	Obtaining communication or other information, including monitoring, observing or listening to a person's communication and other activities, and recording them (s. 99(2) and (4) IPA).	Not as far as is known.
United States	No explicit legislation regarding hacking. If hacking is regarded	Partly direct	No restrictions on the type of offences.	Different operations may be carried out, which can collect	In 2011, 2013, 2014 and 2015, there were only a few federal

Country	Provision hacking power	Direct/indirect powers	Type of offence	Investigative activities	Case law
	as a search under the Fourth Amendment, Rule 41 of the Federal Code of Criminal Procedure (personal communication, 27 June 2022) applies and a warrant must be requested. Half of the judges in the district courts (Škorvánek et al., 2020), who have to give an opinion on the warrant sought, do not consider some hacking activities (depending on the type of data accessed) to be a search under the Fourth Amendment (Mayer, 2018).			various types of data: subscriber information, metadata communications, geolocation data, content of (stored) communications and files. Not all types of data require a warrant under the Fourth Amendment (Mayer, 2018; US v. Jones; Florida v. Jardines; California v. Riley; Škorvánek et al., 2020).	court decisions on government hacking. In 2016 and 2017 combined, there were approximately 100 judgments (Mayer, 2018). On 5 November 2018, there were 17 federal appeal court decisions and numerous federal court decisions in hundreds of different individual prosecutions. All decisions related to two federal child pornography investigations (Škorvánek et al., 2020).
Sweden	Covert Data Reading Act (2020:62) (CDRA).	Direct	Based on Section 4 CDRA, these are offences (including preparatory acts) with a minimum sentence of two years or higher. In addition, offences related to drugs and smuggling are specifically mentioned.	Interception communications, monitoring communications, storing location data, turning on microphones in specific areas (surveillance), other data (interception of login data is mentioned as an example) (s. 2 CDRA).	Two rulings that questioned, among other things, the quality of data. Despite data being incomplete, the court ruled that 'the messages correspond well to reality in terms of time and content'. In both cases, the court rejected the defence's objections (Eskilstuna District Court decision of 26-02-2021 in case B 210-21 & Stockholm District Court decision of 22-04-2021 in case No B 5546-20).
Switzerland	Section 269ter Code of Criminal Procedure (CCP).	Direct	Long list of offences mentioned in Section 286(2) CCP. Including violent offences, deprivation of liberty and offences against sexual integrity.	Interception of telecommunications (sound only, no additional data such as photos).	Not as far as is known.

Appendix 3 Country overview - safeguards data collected

Table B3.1 Overzicht waarborgen ten aanzien van data verzameld met behulp van de hackbevoegdheid

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
Australia	No	Ombudsman supervises the use of powers.	Presence of 'evidence certificates', in which all actions performed by the implementing official are recorded (part 6, division 4 SDA).	No information known	Data must be stored in a secure place and deleted when the case is closed (revised explanatory memorandum).	No information known	If powers are used, notification must be made to inspection, ombudsman & minister (part 6, division 2 SDA).
Belgium	No	Not present	Rules on reporting and filing (s. 46quinquies (5) and (7) CCP; s. 90quater (3) CCP; s. 90sexies (1) CCP; s. 90sexies (4); s. 90septies CCP).	Judicial police officers report in writing to the examining judge at least every five days on the authorisation to be executed (s. 90quater (3) CCP).	A number of records are filed with the registry under sealed cover (s. 90septies (4) CCP). Some records must be destroyed (s. 90septies (3) CCP).	Any person in respect of whom the power of data interception (s. 90ter CCP) has been used must be notified in writing of the nature of the use of the power and the days on which the power was used (s. 90novies CCP). The defendant or a lawyer may request to inspect the data and make a request to add all or part of those data to the file. That request may be rejected (s. 90septies (6) CCP).	Appropriate means are used to guarantee the integrity and confidentiality of (...) communications or data of a computer system (s. 90septies (1) CCP).
Bulgaria	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Canada	No	Not present	Operations that have been carried out are reported in the official report (personal communication, 13 June 2022).	No information known	No information known	After the order has been executed, notice of the execution must be given within a time limit that a court considers reasonable (s. 487.01(5.1) PC). During the hearing, information must be provided on the evidence collected.	No further information

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
						Information needs to be provided with regard to data used to show that someone is guilty or not and with regard to whether rights (in 'Charter of Rights and Freedoms') are breached. A lawyer may question the police during a hearing to see if there has been such a breach (personal communication, 13 June 2022).	
Denmark	No	The Danish Independent Evidence Oversight Board supervises how the police and the Public Prosecutor's Office handle digital evidence. Focus is on the execution process and the quality of digital evidence. The Board does not handle individual cases. Nor does it test individual technical tools (Det Uafhængige Tilsyn med Bevismidler, n.d; personal communication, 22 August 2022). In case of data reading and secret searches, a lawyer is appointed for the person against whom the powers are used before the court makes a decision on the use of the powers. The lawyer must be given the opportunity to express an opinion on the requested use	No information known	No information known	No information known	The lawyer must be notified of all court hearings of the case, may attend them and has the right to inspect the material. He or she is entitled to receive a copy of the material. If the police are of the opinion that the material is of a very confidential nature and that a copy cannot be handed over, the court will decide on the matter (see s. 791b(4) and 799(2) in conjunction with 785 (AJA)). In Denmark, once the use of data reading and secret search has ended, there is an obligation to notify (unless it is an exceptional case) (see s. 791b(4) and 799(2) in conjunction with 788 AJA).	No further information

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
		before the court makes a decision (see s. 791b(4) and 799(2) in conjunction with 784 of the Administration of Justice Act (AJA)).					
Germany	No	The '*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*' (ZITiS) supports and advises federal security services on security tasks in the field of information technology. ZITiS plays a role in research into and development of technical tools (Bundesministerium des Innern, 2017 (the ZITiS Establishment Decree); personal communication, 21 November 2022).	There are rules on reporting when a technical tool is used, see Sections 100a(6) and 100b(4) CCP.	No information known	Technical tools must, according to the state-of-the-art, provide protection against unauthorised use by third parties. Copied data must, according to the state-of-the-art, be protected against any modification, unauthorised deletion and unauthorised access by third parties (s. 100a(5) CCP). The transfer of communications may only take place between the extracting software on the suspect's computer system and the registration and control unit of the executing authority (BKA, 2018 (SLB Directive)).	In Germany notification is required. Notification must take place as soon as possible (unless it is an exceptional case) (s. 101(4) CCP).	In the case of source interception, a technical tool must be installed in such a way that it only records ongoing communications or the contents and circumstances of the communications (s. 100a(5)(1) CCP). Technical tools may only make modifications to the relevant person's computer system and systems that are essential to the data collection (s. 100a(5)(2) CCP). If technically feasible, the modifications made to the computer system must be automatically reversed after the deployment of the powers has ended (s. 100a(5)(3) CCP). Only employees exercising the powers are granted access to the data collected. This must be documented. Moreover, employees are only granted those access rights that are necessary to perform their role. The

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
							software used must be archived (BKA, 2018 (SLB Directive)).
Estonia	No	Not present	All data collected must be stored in a 'processing file' (audio, video, data, etc.). It includes the following elements: 1) name of the organisation using the powers, 2) time and place of the use, 3) name of the data subject, 4) date of the order, 5) only data relevant to fact-finding (s. 126-10 to 126-12 CCP).	No information known	No information known	As a general rule, data subjects are informed after the covert operation has been completed. An exception to this would be if notification could harm the investigation or the investigation methods. When these restrictions no longer apply, a data subject still needs to be informed (s. 126-13 CCP). After notification, the data subject is in principle granted access to the 'processing file' (s. 126-14 CCP). There are exception to this based on s. 126-14 CCP.	No further information
Finland	No	Not present	No information known	No information known	Only the suspect's data may be stored. Other data must be destroyed (email exchange).	No information known	No information known
France	No	In France, STNCJ ('Service technique national de captation judiciaire') is responsible for the design, centralisation and implementation of technical tools used to intercept data. These include technical tools used by the police for hacking. STNCJ is part of the DGSI, a French intelligence agency under the Ministry of	Data used for fact-finding purposes must be transcribed by a judicial police officer (s. 706-102-8 CCP). A report must be drawn up describing the installation of a technical tool. It must include the date and time of the start and end of use (s. 706-95-18 CCP).	Section 706-95-14 CCP regulates that the powers are used under the responsibility of the relevant court (depending on the investigation). They may interrupt the use of the powers at any time. The court must be kept informed of any progress. If it appears that the authorisation and legal requirements are not	Data that has been obtained is stored and sealed (s. 706-95-18 CCP). After the expiry of the time limit, the data is deleted by order of the public prosecutor (Fiche, July 2019, p. 7).	The Act does not include a notification obligation. The defendant is granted access to the data used for the trial.	Devices that are considered a state secret may (also) be used to deploy the powers (Fiche, July 2019, p. 6).

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
		the Interior (Fiche, July 2019).		in order, the use of the powers can be stopped (Fiche, July 2019, p. 6).			
Greece	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Hungary	No	Not present	The use of the powers shall be recorded in minutes or memorandum (s. 243(1) CCP).	No information known	Collected data is provided on a certified data medium. The Special Service for National Security (SSNS) will ensure the integrity of the data collected on the data medium (personal communication, 23 January 2023).	No information known	The SNSS carries out the powers and is responsible for ensuring the reliability, traceability and integrity of the data collected. Exactly what the SNSS does is state secret (personal communication, 23 January 2023). After the powers have been used, the technical tool must be removed (s. 233(1) CCP).
Ireland	No	Not present	No information known	No information known	Data from surveillance under the 2009 Act must be retained for at least 3 years from the end of surveillance (s. 9 Surveillance Act).	Unless proved otherwise, technical tools are presumed to produce accurate information (s. 14(5) Surveillance Act). It is up to the defence to prove that incidents of unlawful conduct have occurred. Unless a court orders otherwise, there is no notification requirement (s. 15 Surveillance Act).	No further information
Italy	No	Not present	A report must be drawn up of all activities (s. 268/269 CCP).	No information known	As a general rule, activities take place by using the Public Prosecution Service's systems, or if these are technically inadequate by using systems of the Criminal Investigation	The defendant has the right to listen back to the recordings or 'take cognisance of computer or telematics communication streams by electronic data transmission	No further information

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
					Department (CID) (as well as the defendant's device) (s. 268/269 CCP). Recordings must be sent immediately to the CID's systems for archiving (s. 268/269 CCP).	means' (s. 268/269 CCP).	
Croatia	No	Not present	The police issue a daily report on the execution of the operations and document technical actions. This report is sent to the public prosecutor (s. 337(1) CCP).	At any time, the examining judge can ask the public prosecutor to report on the course of the use. The examining judge can also request information from the police. The police will eventually draw up a report detailing the start and end time of the use and the data subjects subjected to these powers (s. 337(3) CCP).	The data, report and documentation are kept sealed at the public prosecutor's office. Information not relevant to the investigation is excluded from the file (s. 338(2) CCP). The public prosecutor must hand over the sealed data to the examining judge and an expert assistant will extract the relevant data (s. 338(3) CCP). The collection of digital data should be compiled with certified technical tools to make sure that data is not altered (answer to written questions, 31 October 2022).	The Code of Criminal Procedure (CCP) does not contain a notification requirement (Jurić & Roksandić, 2021, p. 397). However, after it has been carried out, the order may be handed over to the defendant at his or her request (s. 335(5) CCP). At the defence's request, the data must be made available for inspection. After inspection, the data may be listened to or read out during the hearing (s. 338(4) CCP).	There are no specific rules focusing on the admissibility of intercepted or stored electronic communications data. General rules and principles regarding evidence are valid (Jurić & Roksandić, 2021, p. 406).
Latvia	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Lithuania	No	Not present	Data used for fact-finding should be included in the case file (personal communication, 18 July 2018). Only data relevant to the investigation is to be included in the official record. Non-relevant data and data on a common carrier	No information known	No information known	Once the use of the power has ended, persons against whom the power has been used must be informed as soon as possible, but without compromising the success of the investigation, that the power has been used (s. 161(1) CCP).	In exceptional cases, persons other than preliminary judicial investigation officers may conduct the investigation as referred to in section 158 CCP (s. 158(6) CCP). Detailed information on the methods and means used to gather

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
			containing data relevant to the case are not added to the case file and, following a decision by the public prosecutor, are destroyed (s. 158(8) CCP). General safeguards on electronic evidence: a time indication needs to be added to evidence so it is clear when changes were made. Electronic signatures should also be used to make it clear who collected the evidence. Furthermore, professional tools should be used. It is not made clear what is meant by a professional tool (personal communication, 18 July 2018).			A defendant has the right to be granted access to preliminary investigation data, with the exception of personal data. The defendant also has the right to make copies or extracts from the preliminary investigation. A public prosecutor has the right to refuse access to all or part of such data. An appeal may be lodged against this decision (s. 181(1) CCP). If data has been collected and such data is not confirmed and a preliminary judicial investigation is not initiated, but a person has suffered negative legal consequences (as a result of the information that has been collected), then at the person's request, such data must be handed over to the person, with the exception of the data referred to in Section 19(7) of this Act (s. 5(6) Criminal Intelligence Act). During the hearing, the person conducting the investigation may be called as a witness (s. 158(7) CCP).	criminal intelligence, on the tactics used, on the identity of undercover officers and on the composition of the team is not disclosed (s. 19(7) Criminal Intelligence Act).
Luxembourg	No	Not present	An official report needs to be drawn up detailing the actions	No information known	A sealed copy is kept and handed to the judge. The judge may	The defence receives a copy of the data when the case comes up for	Appropriate measures need to be taken to ensure the integrity

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
			taken to install or de-install the software and the actions to transfer computer data (s. 88-4(2) CCP).		have the copy analysed by a technical expert (s. 88-4(3) CCP). Data will be deleted after completion or the period for prosecution expires, unless they are still used for a pending case (s. 88-4(8) CCP).	hearing (s. 88-4(5) CCP). Notification at the start of the court case. The Act makes no mention of notification if no useful evidence has been found (personal communication, 12 July 2022 & 21 July 2022).	and confidentiality of the data (s. 88-4(3) CCP). The Act does not specify the measures to be taken.
Norway	No	A copy of any petition and order of data reading must be sent directly and without delay to the Attorney General, together with the court order and the case's underlying documents (Communication Control Regulation, section 3). There is also a controlling committee charged with checking that the use of communication control, audio surveillance and data reading take place within the framework of the law and instructions, that the use of coercive measures is limited and not used for other reasons than those mentioned in the Criminal Procedure Act sections 216a, 216b, 216m and 216o. The committee may also interview any police and prosecution authority employee, or anyone else assisting with data reading, without limitations of	The police must keep a record of the following: name of the authority using the powers, the request made by the Public Prosecutor's Office, the court order, indication of which computer system the deployment of the power is aimed at and the start and end date of the use of the powers (s. 7(1) Regulations on communication control, room eavesdropping and data reading (*Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing*, hereinafter the Communication Control Regulation). In addition, with regard to data reading, a number of other issues also need to be recorded. These include: the time when equipment was installed and removed, whether technical tools	No information known	The police must try as far as possible to prevent the risk of anyone gaining unauthorised access to the computer system or to protected information, or of anyone committing other criminal offences (s. 216p(2) CCP). Data must be kept in a proper and appropriate manner (s. 8(1) Communication Control Regulation). Data, corresponding to the security instructions, are to be kept where necessary in the context of prevention and investigation. If specifically stipulated, data must be kept in a more secure manner (s. 9(2) Communication Control Regulation). The chief of police ensures the shielding of data when, according to the rules in Section 50(3) of the Police Register Act, they can no longer be	The defendant has a general right to access all 'case documents' established in section 242 and 264 CCP. During the investigations, this access may be restricted when access might damage or endanger the investigation, other investigations or third parties (s. 242 CCP) (personal communication, 26 June 2023). The term 'case documents' includes all evidence documents, maps, photographs, sketches/drawings and audio recordings (CCP s. 242, s. 264 and multiple Supreme Court decisions, e.g. HR-2017-274-U and HR-2017-2145-U). There are, however, restrictions on what the court may receive as evidence, for example, state secrets and information subject to professional secrecy (personal	No further information

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
		confidentiality. Finally, any use of data reading by the Police Security Service (PST) is subject to supervision and review by the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (EOS-utvalget) as directed by the EOS Control Act (personal communication, 26 June 2023)	such as hardware or software were used, whether there was a physical break-in, whether the police broke or bypassed the security of the computer system (s. 7(2) Communication Control Regulation).		kept (s. 9(3) Communication Control Regulation).	communication, 26 June 2023). In Norway, a notification requirement applies after the use of the powers (unless exceptional rules apply) (s. 216o(5) in conjunction with s. 216j CCP).	
Austria	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Poland	No	Not present	No information known	No information known	No information known	No notification obligation.	No specific measures on data quality (Legal Frameworks for Hacking by Law Enforcement).
Portugal	No	Not present	Police officers write a record of the recordings that are relevant as regards the evidence. They describe the content and why it is relevant to uncovering the truth (s. 188(1) CCP). A judge will order that technical materials and reports that are not relevant to the investigation be destroyed (s. 188(6) CCP). The police that has carried out the operation will write a report by 48 hours after the end of it (Article 3(6) Law 101/2003).	Every fortnight, the police must hand over the technical material, recordings and reports to the Public Prosecutor's Office (s. 188(3) CCP). Within 48 hours, the data must be sent to the court (s. 188(4) CCP). Part of the material collected (technical and irrelevant to the case) must be destroyed (s. 188(6) CCP). Furthermore, the court may order the transcription of data only to base its decision on coercive measures (s. 188(7) CCP).	Copies of recordings may be made (s. 187(8) CCP). By court order, technical materials, relating to conversations or communications that have not been transcribed, are kept in sealed envelopes and destroyed after a decision on the case has become res judicta (s. 188(12) CCP). Information from this sealed envelope may only be used in case of an exceptional appeal (s. 188(13) CCP).	The defendant and the party assisting the public prosecutor may access the intercepted communications only after the proceedings become public (s. 188(8) CCP) (personal communication, 12 June 2023). The judge may listen to the recordings to see whether they are correctly transcribed and whether other recordings should be added (s. 188(10) CCP). The judicial authority shall order the report referred to in Article 3(6) to be added to the file only if it deems it absolutely	Section 19 Cybercrime Act: There are no rules in the Act on operational aspects or specific requirements of the powers. No reference is made to technical rules to be observed when obtaining and recording data at the time of using the powers. There are also no rules on the use of malware, such as the type of malware, the installation process and the collection of information (Verdelho, 2021, pp. 1260 and 1261). Act No. 05/2022: The conditions laid down in Section 188 CCP also apply to this Section

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
						indispensable in evidential terms (s. 4(1) Law 101/2001) (personal communication, 12 June 2023)..	(s. 6(3) Act No. 05/2022).
Romania	No	Not present	An official report must include all actions performed and findings revealed (s. 143(1) CCP).	No information known	A copy of all data must be kept in a sealed envelope for consultation by the court (s. 143(2) CCP). An electronic signature based on a certificate issued by an accredited service provider that issues certificates can be used to obtain, send and receive data (s. 142(1) CCP). No further explanation is given of what exactly this entails.	No information known	No further information
Slovenia	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Slovakia	No	Not present	When the data are used as evidence, a verbatim transcript has to be made by someone from the police department who carried out the interception. This should include the facts relevant to the criminal proceedings. Information should also be added about the place, time and authority that made the recording and the lawfulness of the interception (s. 115(6) CCP).	No information known	The data must be stored in their entirety in 'suitable electronic carriers' (s. 115(6) CCP). Hashing is used to store the data (personal communication, 22 August 2022).	Copies may be requested by the public prosecutor, the defendant and/or the defence. The defendant and the defence may also make their own transcript of the data. The court assesses the reliability of the transcript (s. 115(6) CCP).	No further information
Spain	No	Not present	All official reports are included in the file. Should the powers fail	The court must ensure that measures have been taken so data	The making and retention of copies of the data recorded	The defendant is granted access to a copy of the data	The court decision approving the use of the power must state

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
			to produce any evidence, this fact is also mentioned in the file (personal communication, 9 June 2022).	remains intact (personal communication, 9 June 2022). If the power is executed for longer than the period for which consent was given, the examining magistrate may decide that the information collected will be deleted (personal communication, 12 June 2023).	remotely requires separate permission from the court (s. 588(2)(d) CCP). When making copies, precautions must be taken to ensure the integrity and identity of the data. The copies are transferred to the Court's Clerk (Eurojust). The court decision in which approval is given to use the power must describe measures to 'preserve the integrity' of data, as well as measures to ensure the data can be made inaccessible or deleted (s. 588(2)(e) CCP; Eurojust; Ministerio Fiscal, 2019 (Circular)).	collected. When the defendant has received a copy of the data, a third party may be requested to examine the copy (personal communication, 11 July 2022).	the manner in which computer data will be accessed and stored, and the type of software used (s. 588(2)(b) CCP). In case of software, an indication of the programme must be given (to the defense party, if he-she request it (personal communication, 6 juni 2023), which could include the technical or commercial name or the type of programme and the manufacturer. Where programmes specifically created for the police are used, only an indication of the type of programme (such as a Trojan or a keylogger), and if applicable, the potential scope and functionalities of the technical tool, has to be provided. Specific technical data need not be shared (Ministerio Fiscal, 2019 (Circular)).
Czech Republic	No	Not present	If a recording is made during surveillance and that recording is used as evidence, a protocol must be drawn up that meets the conditions of Sections 55 and 55a CCP. Section 55 regulates, among other things, that a protocol is drawn up of all actions carried out. The protocol includes that	No information known	No statutory measures. Police would use hashing and ensure the authenticity of data is technically guaranteed (answer to written questions, 3 January 2023). If nothing substantial emerges from the surveillance, the recordings are destroyed in a	If the police have finished their investigation, and the results are sufficient to fill in a charge sheet, the defendant, the defence and the victim are given the opportunity to inspect the file within a reasonable period of time and submit an application to supplement the	If the recordings reveal information on offences other than those for which the warrant was issued, they may be used as evidence under certain conditions, namely if legal action concerning intentional criminal activity is initiated in respect of that case or if the person whose rights and freedoms

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
			attention is paid to: name of organisations, place, time and subject of the action and an explanation of the actions carried out (s. 55(1) CCP). The remainder of Section 55 CCP mainly concerns the conduct of an interrogation. To record the course of an action, a stenographic record can be made, which can be attached to the report together with, for example, audio and video recordings (s. 55a(1) CCP). If audio or video recordings are made in addition to the protocol, this is noted in the protocol. The technical recording medium is attached to the file and it is indicated where the medium is stored (s. 55a(2) CCP).		prescribed manner (s. 158d(8) CCP). Communications with a lawyer should also be destroyed (s. 158d(1) CCP).	investigation. The police may consider the requested supplement not necessary and reject it (s. 166(1) CCP).	were affected consents to this (s. 158d(10) CCP). Telecommunications operators are obliged to cooperate in surveillance (s. 158d(9) CCP).
United Kingdom	No	There is an Investigatory Powers Commissioner's Office (IPCO). IPCO is responsible for overseeing the use of investigatory powers, including equipment interference: ensuring that they are used in accordance with the law and the public interest (Eurojust). Complaints or disputes on the use of investigative powers,	If data is used as evidence in a criminal proceeding, it must be demonstrated how the evidence was obtained (for the integrity of the evidence) (Eurojust; Home Office, 2018 ('Code of Practice')). The Code of Practice does not specify any methods for maintaining the integrity of evidence but concentrates on potential conflicts with other legislation such	No information known	Section 129(2) of the Investigatory Powers Act (IPA) describes that the following subjects must be limited to the minimum for what is necessary for authorised purposes (these purposes are listed in paragraph 3): o The number of persons to whom the collected material is made public or available. o The extent to which	In the UK, the public prosecutor is as a general rule obliged to disclose under the Criminal Procedure and Investigations Act 1996. The defence is expected to file a defence case statement which includes a justification for specific types of disclosure. If the parties disagree the defendant can apply to the court for disclosure and the court will decide. One ground	Systems used for equipment interference are subject to internal examinations. NCA tools used are confidential (Eurojust). The 'Good Practice Guide for Digital Evidence' prepared by the Association of Chief Police Officer's (ACPO) sets out four principles regarding the forensic examination of digital data:

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
		including equipment interference, can be handled by the Investigatory Powers Tribunal (Eurojust).	as the Computer Misuse Act 1990 and Data Protection Act 2018. There is also a potential conflict with Part 2 of the Investigatory Powers Act which deals with the interception of data in transmission as opposed to data captured from a storage device. The Act says that data caught in transmission is inadmissible, cannot be used as evidence and cannot be referred to (s. 56 IPA) (personal communication, 3 June 2023)		the collected material is made public or available. o The extent to which the collected material is copied. o The number of copies. Copies of collected data should be stored in a secure manner (s. 129(4) IPA). All copies must be destroyed as soon as possible if there are no longer any grounds for keeping them (s. 129(5) IPA).	upon which the prosecution can seek to withhold is Public Interest Immunity – PII. The indications are that most 'equipment interference' activity (EI) in the UK is not produced in evidence but withheld on PII grounds. Very few of these resulted in production as evidence (Sommer, 2022, p. 3) (personal communication, 3 June 2023).	1. No action is permitted that changes evidence data on a digital device. 2. The person using the powers must be competent and able to explain their actions and the implications of those actions to the court. 3. Logging of all processing of digital evidence should be maintained. An independent third party should be able to examine these processes and reach the same conclusion. 4. The officer in charge of the investigation is responsible for ensuring compliance with the law and these principles. (Horsman, 2020; Sommer, 2022).
United States	No	Not present	As a general rule, no information is disclosed about the method used (Gutheil et al., 2017). In case of lawful hacking, 'the inventory' is limited to describing the physical storage of the media that were searched and copied (Rule 41f(1b) Federal CCP).	No information known	The officer may keep a copy of seized and copied electronically stored data (Rule 41f(1b) Federal CCP). The person executing the warrant must return the warrant, together with the inventory, to the examining judge. This can be done through 'reliable electronic means' (Rule 41f(1d) Federal CCP). The judge to whom the warrant is returned will attach to a warrant a certificate of return,	On request, the court will provide a copy of 'the inventory' to the defendant and the applicant for the warrant (Rule 41f(1d) Federal CCP). During legal proceedings, the court may ask the code to be made public. In a specific case that was part of the 'Playpen investigation', the FBI refused to do so and a court dismissed the evidence gathered as a result (Gutheil et al., 2017).	There is no special legislation (other than the conditions that apply when a warrant must be applied for under the Fourth Amendment) guaranteeing constitutional rights that must be respected (Gutheil et al., 2017). However, an amendment to Rule 41 Federal CCP is said to be currently being drafted to ensure that police have to provide more information about their modus operandi. This would

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
					the inventory and all other accompanying documents, and will deliver them to the clerk of the district in which the seizure took place (Rule 41i Federal CCP). Methods need not be specified. A lot of what happens in the field of hacking remains unnoticed by the court. Moreover, court orders often remain sealed (Gutheil et al., 2017).		involve more conditions regarding transparency (personal communication, 27 June 2022). With regard to evidence, and any objections that may be made to it, the general Federal Rules of Evidence apply (personal communication, 27 June 2022). Examples of rules that may apply include the use of an expert witness (Rule 702 Federal Rules of Evidence) and requirements regarding notice in a criminal case by the public prosecutor (Rule 404 Federal Rules of Evidence).
Sweden	No	SIN supervises the use of the powers. The court notifies SIN if the powers are about to be used. Theoretically, SIN can subject any case of which it is notified to its supervision (personal communication, 26 august 2022). If SIN identifies irregularities, it issues a ruling. While SIN's rulings are not binding, in principle, the organisations follow SIN's rulings (personal communication, 29 September 2022).	No information known	No information known	No information known	As a general rule, a person should be notified as soon as possible but no later than one month after the preliminary investigation has been completed (s. 31 Chapter 27 CCP). Notification is not required if the preliminary investigation concerns the offences referred to in paragraphs 1 to 7 (s. 33 Chapter 27 CCP). At a hearing, defendants are granted access to the evidence that has been collected against them.	There are internal police guidelines on the use of technical tools. These are confidential and not publicly available. The police use standardised or certified software whenever possible (e.g. by police abroad) (personal communication, 6 juli 2022).

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
		Besides the judicial review of lawfulness, there are no statutory criteria on which the supervision focuses. The review framework is still a work in progress (personal communication, 26 august 2022).				The suspect can request, substantiated, to view more data (personal communication, November 9, 2022 interview). The public prosecutor may call the police officer concerned as a witness to explain what actions were taken and how the quality of the data is assured (personal communication, November 9, 2022).	
Switzerland	No	Not present	The transmission of data from the defendant's computer systems to the police and the Public Prosecutor's Office ('Strafverfolgungsbehörde') must be secure (s. 269quater(2) CCP). Special software must be used that records the surveillance 'unalterably and without interruption'. The recording is part of the file (s. 269quater(1) CCP). The police draw up a report for the public prosecutor setting out what has been done in using the powers. The report covers such facts as that data have been retrieved, stored and hashed. No information is disclosed on the exact working method of	No information known	Recordings of an authorised surveillance operation that are not necessary for the court case are kept separately from the procedural documents and destroyed immediately after the proceedings have ended (s. 276(1) CCP). Measures are taken to securely transmit data, e.g. using hashing and forensic containers (personal communication, 18 January 2023).	The public prosecutor notifies a defendant of the use of the powers, at the latest after the preliminary investigation has ended (s. 279(1) CCP). Notification is not required (s. 279(2a) and (2b) CCP).	Criminal justice authorities must ensure that the source code can be checked to verify that the software contains only the legally authorised functions (s. 269quater (3) CCP). The police and the Public Prosecutor's Office describe a detailed process of the use and operation of GovWare that also focuses on authorisations (EJPD, 2023).

Country	Examination tools	Supervisory body	Documenting operations & logging	Judicial supervision	Data storage	Trial & right to inspection	Other
			GovWare (personal communication, 18 January 2023). Logging is to ensure that all steps taken are traceable (EJPD, 2023). In practice, it would not involve technical logging, but indicating what kind of data was retrieved (personal communication, 18 January 2023).				

Appendix 4 Detailed country description Netherlands[266]

Statutory regulation
The Computer Crime Act III (hereinafter: the CC Act III) gave authorised hacking a legal foundation in the Dutch Code of Criminal Procedure (Articles 126(nba), 126(uba) and 126(zpa) of the CCP).[267] The new authorisation provides investigating officers with the possibility 'of, under certain conditions, remotely and secretly intruding into a computer system in use by a suspect in the interests of achieving specific objectives when investigating serious criminal offences'. After intruding into ana computer system, police are authorised to perform a number of investigatory procedures, namely:

- determining and documenting specific characteristics of the computer system or the user, such as identity or location;
- executing an order to record confidential communications (Art. 126(l) of the CCP) or wiretapping and recording communications (Art. 126(m) of the CCP);
- executing a continuous surveillance order (Art. 126(g) of the CCP);
- documenting information that is present or stored in the computer system;
- rendering data inaccessible, e.g. by dismantling a botnet.[268]

The CC Act III contains several other grounds which can be used as the basis for establishing rules regarding the implementation of authorised hacking under or pursuant to a General Order in Council. This law formed the basis, for example, of the Decision on intruding into automated information systems (hacking), hereinafter: the Decision.

Competent authorities
Various levels within the Public Prosecution Service are involved in oversight of the deployment of authorised hacking, both prior to deployment as well as while the police action is being carried out. Some areas of this involvement follow logically from Articles 126(nba), paragraph 1 of the CCP. The public prosecutor draws up a demand for authorised hacking for the examining magistrate, and subsequently, when the demand is granted, an order for the police. The national public prosecutor, who is responsible for these authorisations in his or her portfolio, is involved at an earlier stage (*Parliamentary Papers I*, Actions 19 June 2018, no. 34, p. 19). This public prosecutor gives direction to the police team that will be implementing the authorised hacking. Before the public prosecutor can issue a final demand for authorised hacking, the proposed police action is submitted to the Central Assessment Committee (CTC).[269] The CTC subsequently issues its opinion to the Board of Procurators General,[270] who take the final decision. A justification criterion is included in these deliberations.[271]

[266] This chapter is based on – and largely adopted from – the report on implementation of authorised hacking in the Netherlands (Van Uden & Van den Eeden, 2022).
[267] Articles 126(nba), 126(uba) and 126(zpa) of the CCP.
[268] A botnet is a network of internet-connected compromised computer systems (or other systems) that are remotely controlled (Van der Waagen & Bernaards, 2018, p. 59). These networks are used to disseminate malware (Van der Waagen & Bernaards, 2018, p. 60), which can perform such actions as recording a computer user's keystrokes (*Parliamentary Papers* II 2015/16, 34 372, no. 3, p. 22).
[269] The CTC is an internal advising body within the Public Prosecution Service. Committee members assess the legality of the action based on legislation and regulations, case law, proportionality, subsidiarity and potential risk factors. In addition, the CTC weighs the effectiveness of the authorisation and the risk factors against the importance of granting the authorisation in any given case.
[270] *Parliamentary Papers II* 2015/16, 34 372, no. 3, p. 38.
[271] *Parliamentary Papers I* 2016/17, 34 372, D.

After the Procurator General has approved a potential police action using authorised hacking, the public prosecutor submits a demand for authorisation to the examining magistrate. The examining magistrate rules on such actions in terms of whether they could form a breach of privacy or whether there is any risk to the integrity and maintaining control of the investigation.

The actual implementation of authorised hacking is in the hands of specially appointment investigating officers (Digital Police), who form part of a specialised team of the National Unit (Landelijke Eenheid) of the National Police. Currently, this is the only police team in the Netherlands that implements authorised police intrusion. The results of the authorised police intrusion are transferred to the tactical investigating team conducting the police investigation.[272]

Against whom?
An authorised police action must be performed in a targeted way. That means permission to intrude into an automated computer system in use by a suspect or suspects.[273] An order may pertain to multiple computer systems, provided the suspect uses the computer systems and that intrusion is deemed necessary for the investigation of criminal offences.[274]

Cases
The authorisation may be used, first, to investigate offences as referred to in Article 67(1) of the CCP, referred to as preventive detention offences, as well as for offences that result in a serious breach of rule of law.[275] Second, the authorisation is intended for an investigation into persons for whom a reasonable suspicion exists that they are occupied with planning and/or committing organised crime.[276] Third, the authorisation is permitted to be used when there are clues pointing to an act of terrorism.[277] Depending on the objective of the investigation envisaged by the investigation agencies, a fourth and fifth criterion may be applicable. If the aim of the investigating agencies is to secure information[278] and/or to render it inaccessible,[279] the alleged offence must carry a prison sentence of eight years or more as codified in law. Deployment of such police actions are also permitted for investigations into crimes for which a General Order in Council has been issued. These concern offences that do not carry a prison sentence of eight years or more, but have been committed with automated computer systems and have an automated computer system as their objective.[280] The Decision also stipulates serious joint offences, which are increasingly committed with the aid of a computer system. What all these crimes have in common is that frequently there are no other means of access for investigating the computer system that is being used to commit the crime.[281] Moreover, there is a clear public interest in terminating the criminal situation and prosecuting the offenders.[282]

[272] Decision on intruding into automated information systems (hacking), p. 14.
[273] Article 126(nba), paragraph 1 of the CCP.
[274] *Parliamentary Papers II* 2015/16, 34 372, no. 6, p. 13.
[275] Article 126(nba) of the CCP.
[276] Article 126(uba) of the CCP.
[277] Article 126(zpa) of the CCP.
[278] Article 126(nba), paragraph 1, subparagraph D of the CCP.
[279] Article 126(nba), paragraph 1, subparagraph E of the CCP.
[280] Decision on intruding into automated information systems (hacking), 2018, p. 2. An example of such a crime is intentionally and unlawfully copying non-public data stored by means of an automated information system (Art. 138(c) of the CCP).
[281] Decision on intruding into automated information systems (hacking), 2018, p. 11.
[282] Decision on intruding into automated information systems (hacking), 2018, p. 11.

Term of authorisation
The authorisation is granted for a maximum period of four weeks. This period can be extended indefinitely by up to four weeks.[283] No maximum period has been set for making use of the authorisation. Nor is there any maximum number of extensions. The Digital Police will terminate their investigation when they have achieved the objective of the intrusion into a computer system or when the period of validity of the order has expired.

Formalities
An order for an action for authorised hacking must be issued in writing; at a minimum the order must include the following topics:[284]

- the offence and the name of the suspect, if known, or otherwise the most precise description of the person possible;
- where possible, a number or some other means by which the computer system can be identified, and, if known, an indication that the data is not stored in the Netherlands;
- the facts and circumstances indicating that the conditions, referred to in Article 126(nba), paragraph 1 of the CCP, have been satisfied;
- an identification of the nature and functionality of the technical tool, as referred to in Article 126(nba), paragraph 1 of the CCP, that will be used to implement the order;
- the section or sections, referred to in Article 126(nba), paragraph 1 of the CCP, that form the grounds on which the order has been issued, and – if this pertains to paragraphs (a), (d) or (e)[285] – a clear outline of the actions to be performed;
- which part of the computer system and which category of data the order permits access to;
- the time at which, or the period within which, execution of the order will be carried out;
- if it concerns an order as referred to in Article 126(nba), paragraph 1(c) of the CCP,[286] a statement of the intention of planting a technical device on a person.

An order can only be issued following a written authorisation handed down by the examining magistrate, after the public prosecutor has submitted a demand for authorised intrusion. The authorisation must refer to all the required parts of the order and the period for which the authorisation is valid.[287] In cases of utmost urgency, the public prosecutor's decision and the examining magistrate's authorisation may be given orally. In which case, however, the public prosecutor and the examining magistrate must record their decisions in writing within three days.[288]
Article 126(nba), paragraph 8 of the CCP stipulates that rules will be set by or pursuant to a General Order in Council regarding a) the authorisation and expertise of the investigating officers who will be tasked with intrusion and investigation, as referred to in Article 126(nba), paragraph 1 of the CCP, and collaboration with other investigating officers; and b) the automated documentation of data regarding execution of the order, as referred to in Article 126(nba), paragraph 1 of the CCP.
Lastly, Article 126(nba), paragraph 9 of the CCP contains an outline of the rules that

283 Article 126(nba), paragraph 3 of the CCP; *Parliamentary Papers II* 2015/16, 34 372, no. 3, p. 54.
284 Article 126(nba), paragraphs 2(a) through (h) of the CCP.
285 Subparagraph (a) refers to determining and documenting specific characteristics of the automated information system or the user, such as the identity or location; subparagraph (d) refers to documenting information that is present or stored in the automated information system; and subparagraph (e) to rendering data inaccessible.
286 The enforcement of a continuous surveillance order (Art. 126(g) of the CCP).
287 Article 126(nba), paragraph 4 of the CCP.
288 Article 126(nba), paragraph 5 of the CCP.

can be set for application of the authorisation, as referred to in Article 126(nba), paragraph 1 of the CCP, for cases in which it is not known where the data is being stored. The procedure to be adopted when a computer system is located abroad is outlined in the Instructions for International Aspects of Assigning Authorisation.[289]

Technical tools

In order to conduct investigatory actions, technical tools may be used. A technical tool is a 'software application that detects, registers and transports data, and with which investigatory actions can be conducted in execution of an order' (Decision on intruding into automated information systems (hacking), 2018, p. 2). It is not 'strictly necessary' to make use of technical tools. Actions will sometimes be performed in an 'ad hoc and manual'[290] way.[291]

Technical tools have one or more functions, such as taking screenshots, recording sound, recording keystrokes and/or searching through file folders in order to find and record data. The required functions must be laid down in the public prosecutor's order, and during the investigation the technical tool must be set up in such a way that only the functionalities outlined in the order can actually be used.[292] Data that is collected will be sent to the technical infrastructure[293] of the police.[294] The technical infrastructure is the storage location for data recorded during execution of the order.[295]

Safeguards

Requirements for technical tools

The Decision sets a number of requirements for technical tools. Some of these requirements focus on promoting the reliability, integrity and traceability of data. These three areas can be defined as follows based on the Decision.[296] Reliability means that data contained in a computer system and data that is registered by a technical tool must be exactly the same. Integrity indicates that the operation of a technical tool does not change and that the registered data does not change. Integrity also means that no unauthorised persons have access to the data. Finally, traceability means that it is clear that the registered data were obtained from the technical tool used by the suspect.

The Decision lays down that a technical tool must at the very least meet the following requirements:

- A technical tool must be set up in such a way that the operation thereof can be restricted to the functionality or functionalities that have been stated in the order (targeted operation).[297]
- A technical tool only detects and registers data for the purpose of the functionality or functionalities stated in the order (targeted detection and registration).[298]

[289] Government Gazette, 26 February 2019, no. 10277.
[290] For ease of reading, this chapter does not discuss how investigatory actions are conducted in ad hoc and manual ways.
[291] Decision on intruding into automated information systems (hacking), 2018, p. 16.
[292] Decision on intruding into automated information systems (hacking), 2018, p. 37, Article 8 of the Decision.
[293] Technical infrastructure refers to a 'technical provision of a technical team intended for recording data pursuant to execution of an order' (Decision on intruding into automated information systems (hacking), 2018, p. 2).
[294] Article 13, paragraph 1 of the Decision.
[295] Decision on intruding into automated information systems (hacking), p. 33.
[296] These definitions have been inferred from the Decision because the Decision does not contain specific definitions of these terms.
[297] Article 8 of the Decision.
[298] Article 9, paragraph 1 of the Decision.

- A technical tool that has one or more functionalities for the purpose of recording telecommunications only detects and registers communications that take place using one or more identifiable characteristics of the computer system of the individual user or users to whom the order pertains (targeted detection and registration).[299]
- A technical tool registers data in such a way that the contents of the registered data are identical to the contents of the detected data (reliability and integrity).[300]
- A technical tool is protected against changes in its operation, against changes in the registered data and against access of the registered data by unauthorised persons (reliability and integrity).[301] These requirements pertain to the security measures that protect a technical tool from external influence as much as possible according to the 'state of technology'. This might include such things as authentication measures for communicating with the technical tool or encrypting data by means of a digital signature. The latter ensures that the data registered by the technical tool is unreadable and inaccessible.[302]
- A technical tool provides the registered data with a unique identifier (traceability).[303] This identifier must reveal the relationship to the technical tool that is being deployed. An example of a unique identifier is a code that is added when deploying the technical tool.[304]
- A technical tool provides the registered data with the date and time at which registration took place (date and time).[305] This means that there is certainty about the date and time at which the technical tool registered the data as soon as the data has been registered.[306]
- A technical tool automatically transports the registered data to the technical infrastructure of the police (transport).[307]
- A technical tool protects the registered data during transport to the technical infrastructure against changes to the registered data and against access of the registered data by unauthorised persons (transport).[308]

In addition, Article 22 of the Decision stipulates that the Chief of Police should assign one or more officers who are responsible for the central registration of who can access the technical tool. That same article also stipulates how transfer of the technical tool to the person who will actually implement the authorisation takes place, and what has to be registered in terms of the technical tool that will be transferred.
The data collected must, in principle, be transported directly to the technical infrastructure of the Digital Police.[309] Only officers who have been assigned by the Chief of Police have access to this infrastructure.[310] When recording the data, measures must be taken to prevent changes to the recorded data or access of the recorded data by unauthorised persons. In addition, it must be possible to determine afterwards whether any changes or access of the data have taken place.[311]

299 Article 9, paragraph 2 of the CCP.
300 Article 10, paragraph 1 of the Decision.
301 Article 10, paragraph 2 of the Decision.
302 Decision on intruding into automated information systems (hacking), p. 39.
303 Article 11 of the Decision.
304 Decision on intruding into automated information systems (hacking), p. 39.
305 Article 12 of the Decision.
306 Decision on intruding into automated information systems (hacking), p. 39.
307 Article 13, paragraph 1 of the Decision.
308 Article 13, paragraph 2 of the Decision.
309 Decision on intruding into automated information systems (hacking), 2018, p. 40; Article 27, paragraph 1 of the Decision.
310 *Parliamentary Papers I* 2016/17, 34 372, D, p. 41, and Article 28, paragraph 2 of the Decision.
311 Article 28, paragraph 3 of the Decision.

After completion of the police action, the technical tool will be – to the extent possible – erased, so that the police can no longer use it to receive data.[312] A situation could arise in which a decision is made not to erase the technical tool or not to disable the changes made to the computer system. Such a decision would need to be justified by compelling interests. This might include such things as the genuine chance that erasing it would entail a serious risk to the computer system on which the technical tool was deployed. Should a technical tool not be completely erased, the Digital Police would then be responsible for ensuring that the law enforcement agencies can no longer received data from that computer system.[313] Moreover, the public prosecutor will inform the administrator of the computer system and provide information which would allow erasure of the software or any traces thereof.[314] An official police report is required for erasing a technical tool or for the fact that transport of data has been terminated.[315] It will be possible to check whether the technical infrastructure has actually stopped receiving data based on logging events in the computer system. The erasing process forms part of the Inspectorate's oversight responsibilities.[316] The section on external oversight provides an explanation of the role of this Inspectorate. The recorded data will ultimately be released to an investigating officer who has been tasked with the criminal investigation.[317] If it is necessary for the implementation of the order or for the criminal investigation that a selection be made of the data recorded in a technical tool, the investigating officer of the Digital Police will carry out this procedure. In doing so, he or she will use a copy of the data recorded under Article 27 of the Decision. When making a selection of data, the investigating officer of the Digital Police will document the procedure used for processing the copy of the recorded data in an official police report. This official police report will then be sent to the public prosecutor.[318]

Examining the technical tool

A technical tool must be examined before it can be used.[319] If the technical tool is approved for use, it may be assumed that the legal requirements regarding reliability, integrity and traceability of data have been met.[320] The Dutch National Examination Service is responsible for the examination.[321]

The way in which the examination will be carried out is laid down in a examination protocol,[322] which is not in the public domain. The protocol also contains the criteria that will be used during the examination. The Examination Service and the Public Prosecution Service are jointly responsible for drafting a protocol that the Minister of Justice and Security must approve prior to its use.[323]

As previously mentioned, the Decision contains rules formulated in respect of the technical requirements that have been set for a technical tool and how it should be examined.[324] When examining the software, all the parts of the technical tool that are important for 'detection, registration and transport of data' must be checked.[325] The Digital Police's technical infrastructure is not subject to examination and approval,

312 Article 126(nba), paragraph 6 of the CCP; *Parliamentary Papers II* 2015/16, 34 372, no. 3, p. 36.
313 *Parliamentary Papers II* 2015/16, 34 372, no. 3, p. 36; Article 26, paragraph 1 of the Decision.
314 *Parliamentary Papers II* 2015/16, 34 372, no. 3, pp. 36-37; Article 26, paragraph 2 of the Decision.
315 Article 26, paragraph 3 of the Decision.
316 Decision on intruding into automated information systems (hacking), 2018, p. 47.
317 Article 29, paragraph 1 of the Decision.
318 Article 29, paragraph 3 of the Decision.
319 Article 14 of the Decision.
320 Decision on intruding into automated information systems (hacking), p. 19.
321 Article 14, paragraph 1 of the Decision.
322 Article 17, paragraph 1 of the Decision.
323 Decision on intruding into automated information systems (hacking), 2018, p. 42.
324 Articles 8 through 20 of the Decision.
325 Decision on intruding into automated information systems (hacking), 2018, p. 42.

however.[326] Further, examination is intended to be carried out by 'trial-and-error'.[327] The expectation is that this examination may take several months, which will certainly be the case if the software needs to be modified to meet the final approval.[328] When the examination has been completed, the Examination Service must record its findings in an examination report[329] and include a unique examination approval number.[330] The assumed advantage of such a unique number is that it obviates the need to report any information about the precise operation of the technical tool in the criminal investigation file. This reduces the chance of violations to the integrity of the investigation. Moreover, lawyers and judges are given the guarantee that the technical tool deployed has met all the legal requirements.[331]
In principle, a technical tool is only approved when *all* the requirements set in Articles 8 through 13 of the Decision have been met.[332] However, this may not be possible in all cases. In which case, substitute safeguards will have to be put in place.[333] If a case arises where law enforcement action is performed without a technical tool, other procedural precautions will have to be taken,[334] such as audiovisual recording of the intrusion processes.[335] The period for which the examination report remains valid will be indicated in the report.[336] If within the set period the operation of a technical tool or any part thereof changes such that it no longer meets the stipulated technical requirements, the software must be examined and approved again.[337] The Inspectorate oversees compliance with the requirements of the examination procedure.[338] In principle, law enforcement must make use of a technical tool that has been examined and approved in advance.[339] However, retroactive examination and approval is also a possibility.[340] In addition, it may be that the nature of a technical tool stands in the way of examination and approval.[341] When the latter is the case, the public prosecutor must note down in the court documents that examination and approval has been waived. He or she must also note what kind of additional safeguards have been taken[342] in order to 'guarantee reliability, integrity and traceability of recorded data' (Decision on intruding into automated information systems (hacking), p. 21).

Logging computer operations
Logging or the continuous recording of intrusion operations performed is another way of safeguarding the reliability, integrity and traceability of evidence. The Decision differentiates between four different types of logging:[343]

1 Logging actions: this type of logging pertains to the automatic recording of the screen and keystrokes of the investigating officer of the Digital Police. This type of logging also concerns communications between the technical infrastructure and the computer system, the scripts and software versions in use, and the logbook maintained by the investigating officer. In principle, the intention is that everything

[326] Decision on intruding into automated information systems (hacking), 2018, p. 42.
[327] Decision on intruding into automated information systems (hacking), 2018.
[328] Decision on intruding into automated information systems (hacking), 2018, p. 40.
[329] Article 18, paragraph 2 of the Decision.
[330] Article 18, paragraph 3(b) of the Decision.
[331] Decision on intruding into automated information systems (hacking), 2018, p. 43.
[332] Article 14, paragraph 2 of the Decision.
[333] Article 18, paragraph 3(e) of the Decision.
[334] Article 21, paragraph 5 of the Decision.
[335] Decision on intruding into automated information systems (hacking), 2018, p. 45.
[336] Article 18, paragraph 3(g) of the Decision.
[337] Article 14, paragraph 3 of the Decision.
[338] Decision on intruding into automated information systems (hacking), 2018, p. 43.
[339] Decision on intruding into automated information systems (hacking), p. 21.
[340] Article 15, paragraph 1 of the Decision.
[341] Article 21, paragraph 4 of the Decision.
[342] Article 21, paragraph 4 of the Decision.
[343] Decision on intruding into automated information systems (hacking), 2018, pp. 17-18.

is recorded automatically. Should that not be possible, then within the police organisation it must be documented that logging has been conducted manually.
2 Evidence logging: this is one component of the logging actions discussed above. Evidence logging covers recording data during the intrusion stage, whether or not with the aid of a technical tool. These are data that can be used in a criminal case.
3 System logging: this type of logging pertains to logging that was already effected by all the systems in use, which data are collected and recorded at the central level. The aim of system logging is to help flag and solve problems pertaining to the reliability, integrity and accessibility of the technical infrastructure.
4 Authentication and authorisation logging: a component of system logging that concerns access to a technical tool.

External oversight

Inspectorate of Justice and Security

In addition to the examination carried out by the Examination Service, the Inspectorate maintains 'system oversight' of how the authorised intrusion is implemented;[344] the Inspectorate oversees the way that the police perform their task.[345,346] As part of this role, they also oversee 'the functioning of the legal system governing implementation of an order to investigate a computer system'.[347] The Inspectorate is empowered to decide how it wants to perform this oversight and is not dependent on external reporting of problems.[348] A number of different aspects are included in the Inspectorate's powers of oversight.[349] It is, for example, required to monitor the authorisation of the designated investigating officers, including their expertise and depth of knowledge; the deployment of the technical tool, including the question of whether data is processed with due care and within the existing frameworks;[350] compliance with technical requirements and the examination procedure;[351] logging and protection of data; and the way in which the data are used, stored and erased.[352] Oversight not only targets the stage following the investigatory intrusion, the Inspectorate can also randomly monitor the actual intrusion in practice and perform an investigation into a computer system.[353] The Inspectorate will compile its findings annually in a publicly accessible report.[354] If any structural problems are identified, it can ask the law enforcement agency to draw up a 'plan for improvement'. It may also decide 'to intensify' oversight in some areas.[355]

The Inspectorate's tasks are dedicated to the implementation, i.e. has the police action proceeded according to the 'relevant laws and regulations and within the framework of the order issued by the public prosecutor and the authorisation handed down by the

344 *Parliamentary Papers II*, Actions 13 December 2016, no. 34.
345 One reason this system oversight was put in place was the Council of State's expectation that courts will not always be sufficiently capable of making a judgment on how the investigation was conducted. Moreover, not all cases for which authorised hacking has been assigned will be brought before a court (*Parliamentary Papers II* 2015/16, 34 372, no. 4, p. 8).
346 *Parliamentary papers* II 2016/17, 34 372, no. 6.
347 Decision on intruding into automated information systems (hacking), 2018, p. 23; Article 126(nba), paragraph 7 of the CCP.
348 *Parliamentary Papers II*, Actions 13 December 2016, no. 34, p. 47.
349 Decision on intruding into automated information systems (hacking), 2018, pp. 23-24.
350 *Parliamentary Papers* II 2017/18, 34 372, no. 27.
351 Decision on intruding into automated information systems (hacking), 2018.
352 *Parliamentary Papers I* 2016/17, 34 372, D.
353 Decision on intruding into automated information systems (hacking), 2018, pp. 24.
354 Inspectorate of Justice and Security (2020); Inspectorate of Justice and Security (2021); Inspectorate of Justice and Security (2022).
355 *Parliamentary Papers I* 2017/18, 34 372, G.

examining magistrate'?,[356] but it does not assess the justification for the action itself. This is the responsibility of the judge at the court session.[357]

Procurator General at the Supreme Court
The Inspectorate is also not responsible for overseeing the procedures of the Public Prosecution Service; this is the task of the Procurator General at the Supreme Court. The Inspectorate can inform the Procurator General at the Supreme Court if there is any evidence of 'violations of legal requirements by or at the behest of the public prosecutor'.[358] In September 2022, the Procurator General at the Supreme Court published a first oversight report that investigated the Public Prosecution Service's procedures and application of authorised hacking (Aben & Luining, 2022).

Notification obligation and official reports
Following from regulations requiring notification of special investigatory authorisations,[359] authorised hacking carries the obligation of informing the parties involved that the authorisation has been deployed. That means that persons whose computer systems have been intruded upon must be informed that they have been subjected to a police action.[360] Even if the computer system intruded upon is in a foreign country, notification is – in principle – required.[361] Notification is not required if the official report of execution of the authorisation is attached to the court documents.[362]

The Decision lays down which activities the public prosecutor should include in an official report: 1) any irregularities that may have occurred during data collection;[363] 2) deployment of the technical tool, including any irregularities;[364] 3) execution of the investigatory actions, including any irregularities;[365] 4) erasing the technical tool;[366] 5) incomplete erasing of the technical tool;[367] and 6) selection of data, if processing of data has taken place.[368] The aim is to record the actions that the Digital Police conduct 'as quickly as possible' in an official report.[369] In order to protect methods of investigation from disclosure, a less detailed form of accountability may be chosen; it is up to the public prosecutor to make a judgment on this.[370]

Case law
In the period between March 2019 and March 2021, 26 orders were issued for deployment of authorised hacking investigations (Van Uden & Van de Eeden, 2022, p. 12). As far as is known, deployment of authorised hacking has not (as yet) been a subject of discussion during the legal proceedings in a court of law. A couple of cases in which an attempt was made to deploy authorised hacking or in which authorised hacking was actually deployed have been substantively addressed in court (see for example Berndsen, 2022).

356 *Parliamentary Papers I* 2017/18, 34 372, G.
357 *Parliamentary papers* II 2016/17, 34 372, no. 6.
358 *Parliamentary Papers* II 2016/17, 34 372, no. 6.
359 Article 126(bb) of the CCP.
360 *Parliamentary Papers II* 2015/16, 34 372, no. 3, p. 40.
361 *Parliamentary papers* II 2016/17, 34 372, no. 6.
362 *Parliamentary papers* II 2016/17, 34 372, no. 6.
363 Article 6, paragraph 2 of the Decision.
364 Article 23, paragraphs 3 and 4 of the Decision.
365 Article 24, paragraphs 2 and 3 of the Decision.
366 Article 25, paragraph 3 of the Decision.
367 Article 26, paragraph 3 of the Decision.
368 Article 29, paragraph 3 of the Decision.
369 *Parliamentary Papers II* 2016/17, 34 372, no. 3, p. 78.
370 Decision on intruding into automated information systems (hacking), p. 22.

Approval in practice

An important catalyst for conducting this comparative law study was the first report issued by the Inspectorate, on the basis of which the Minister of Justice and Security concluded that the deployment of technical tools, their examination and approval did not yet accord with the intentions of the legal framework. Since then, a first evaluation by the WODC (Research and Documentation Centre) has provided more clarity on the questions of how examination and approval are conducted in practice, and what obstacles police investigators experience in practice when technical tools are examined and deployed. In this section, we set out the most important findings in this context. An overview of these issues is important in order to make a meaningful comparison between the Netherlands and other countries (see Chapter 4).

At the present time, the Dutch National Examination Service (hereinafter: the Examination Service) examines and approves the technical tools developed by the police. This authority operates independently, but forms part of the National Unit (Landelijke Eenheid) of the National Police Board, as does the Digital Police. The Examination Service also examines and approves the more traditional technical tools, such as those referred to in the Decision on technical tools in criminal procedure. This would include trackers that are planted on cars or cameras used to observe suspects. When examining and approving technical tools that are intended for authorised intrusion, the Examination Service follows a examination protocol based on the Decision. This protocol encompasses 17 requirements, each one comprising multiple standards. The protocol contains 56 standards in total. The complete examination protocol is not in the public domain, but one issue the protocol addresses is how transport protection must be set up.

Examination of in-house technical tools

The Digital Police have made use of a technical tool developed in-house, by the police themselves, a few times over the past two years. For the majority of intrusion investigations, a commercial product was used (more on this below). In the period we studied – from March 2019 through April 2021 – three technical tools were developed, two of which were approved by the Examination Service.[371] Developing a good technical tool that meets approval standards takes a great deal of time. Developing the first version of a technical tool can easily take four weeks – and that is for a less complex technical tool. When the technical tool is ready, it still has to be examined and approved. That procedure also takes a minimum of four weeks, but usually requires more time, even though examination and approval proceeds more quickly now than when the law first came into force. Because it has not yet happened that a technical tool was examined and approved on the first try, one or more versions have to be developed subsequently, with a new examination and approval procedure for each new version. All together it takes at least four months to have a tool approved, or it is quite possible that no approval ifs obtained. In practice, therefore, it has proved difficult to deploy a pre-approved tool. The Digital Police are struggling with the fact that a tool that has been modified has to go through the whole examination process again. The Examination Service examines and approves a modified tool again because only then can judgments be made about the operation of the tool and about the question of whether the data it has collected pass the examination of reliability, integrity and traceability.

[371] In its third Annual Report (2022, p. 7), the Inspectorate of Justice and Security writes that in two cases the Digital Police deployed a pre-approved technical tool. In addition, in 2021 seven technical tools were submitted for examination and five technical tools were approved.

Apart from the time requirements, the examination in general forms a more significant obstacle for the Digital Police. This is related to the fact that the Examination Service and the Digital Police view the examination process from two completely different perspectives. From the Examination Service's perspective, it's the rules and regulations that have primacy: as can be deduced from the legal framework, a technical tool can only be approved if it meets *all* the requirements of the examination protocol, potentially augmented with substitute safeguards. This is the prime consideration of the Examination Service because this is how the reliability, integrity and traceability of data can be guaranteed. The Examination Service wants to be able to explain to the court that nothing in the data obtained from a suspect has been changed, which can only be guaranteed if all the requirements have been met.

From the perspective of the Digital Police, the examination is seen primarily in terms of enforcement, and the necessity of the rules and requirements based on those rules. For the Digital Police, the rules and requirements are difficult to execute, among other things because they are often found to be not well suited to the technical tool the law enforcement agency has developed. Their reasoning is that the rules in the Decision, and the examination protocol based on the Decision, mainly take their legal grounds from the 'old' Decision, which was geared towards traditional technical tools, which tools do not primarily consist of software. By primarily taking the 'old' Decision as the basis, policy makers seem to be assuming that the Digital Police are able to gain complete control of the digital environment in which a technical tool will be planted, similar to a tracker, where the police can control the settings and parameters. But it is far from true in practice that law enforcement investigators can take control of a remote digital environment or the operations that a suspect performs within it. For example, the Digital Police cannot control the settings of the suspect's computer system[372] or decide what kind of connection the suspect should use for obtaining data. Furthermore, the Digital Police cannot exercise any influence over what suspects do with their computer systems. If a suspect decides to turn off the computer system, it is problematic for time registration and logging, which really should be operating continuously. This leads to difficulties in demonstrating that the quality of the data collected is trustworthy.

Nor do the Digital Police see all the rules as necessary, because in their view not enough consideration has been given to risk analyses and evidential value. Working on the basis of a risk analysis means making an assessment of the consequences that would ensue if that technical tool did not meet one or more requirements. This would not always be a problem, the Digital Police argue, for example when there is only a very small chance that not completely satisfying a requirement would form a risk to the quality of the evidence being collected. The Digital Police believe, moreover, that 100% reliability should not be pursued at any cost, because evidence will be weighted in different ways. Not all the data that is collected by means of an authorised intrusion investigation (special or otherwise) will be used as evidence, for example, information on data management and administration. Should the data be used as evidence, then it is well to note that suspects are usually convicted on the basis of various pieces of evidence, often collected under a variety of investigatory powers (special or otherwise) assigned to the law enforcement agency. Not all pieces of evidence will possess the same evidential value.

[372] Consider, for example, the time and date settings of an automated information system.

Examination and approval of commercial products
The majority of police investigations where authorised intrusion is deployed make use of a commercial product, the current nature of which, according to a decision of the national Digital Police public prosecutor, stands in the way of examination and approval. The public prosecutor's decision rests on a number of arguments. First of all, the speed of product updates is problematic. On average, a new update is issued roughly every six to eight days. The question then becomes, which version or versions should the Examination Service approve? And if all the versions were to be approved, it would exceed the usual lead time needed for examination and approval. Secondly, the supplier's stance when it comes to business secrecy is problematic. In practice, operation of a commercial product is a 'black box' for police investigators. This means that the Examination Service, too, cannot gain any insight into the operation of the product. The third argument relates to the fact that the supplier wants to have access to the product at all times, to do things like perform maintenance, for example. As a result, the Examination Servicedoes not have exclusive access to the tool, which is required so that it can carry out its examination. The last point in particular is probably responsible in large part for preventing the product from being approved under the current examination regime. That's because the tool makes use of a server that the supplier has access to. Although it's true that the data collected, such as the suspect's chat messages, are ultimately stored on the server of the Digital Police, this does not detract from the fact that, during the intrusion and performance of investigatory actions, the supplier also theoretically has access to the suspect's data. Even though contractual obligations are concluded with suppliers prohibiting their access to this data and only allowing access to the server for maintenance of the product, it cannot be ruled out that a supplier might give itself access to the server at other times. This alone is reason enough to block the approval of a tool. The Digital Police argue that a supplier will never give itself access to the server access this data because there is too high a risk of reputational damage, while the financial penalties this might entail are prohibitive. Nonetheless, this loophole means that the reliability and integrity of the data collected cannot be guaranteed.

If the Digital Police public prosecutor decides that the current nature of the technical tool stands in the way of examination and approval, as mentioned above, other safeguards must be put in place to ensure that the evidence is reliable. The commentary on the Decision reveals that predominantly technical safeguards are implied. Such additional safeguards must be justified by the public prosecutor in the case file. An example of a technical safeguard is enforcing the four-eye or double approval principle. In practice, however, police investigations already provide not only additional technical safeguards, but additional tactical safeguards as well. The latter type of safeguard refers to measures taken by a tactical team to verify data obtained with a technical tool that has not been examined and approved. What kind of verification method or methods are chosen depends on, among other things, the kind of investigatory actions the Digital Police are performing. A verification method can usually refer to one or more methods of investigation (special or otherwise) used by the tactical team simultaneously or just after a police action by the Digital Police. The primary aim of these methods is to establish that the computer system that has been penetrated belongs to the suspect. In addition, in the majority of cases, they also allow something to be said about the contents of the data, for example whether the data collected using different methods of investigation (special or otherwise) corroborate each other. One method of verification used is seizing the suspect's computer system. This allows the Digital Police to compare the data collected with the data that is still stored in the computer system that has been seized. One

disadvantage of this method is that law enforcement agencies will not always be able to gain access to the computer system and/or the necessary data. Another verification method is deploying an observation team. The team can, for example, carry out surveillance in order to find out when the suspect is using the computer system. This information can subsequently be compared with the times that the Digital Police received data from the computer system. The Decision on which the exmination and approval protocol is based does not take into account these kinds of tactical measures that are or can be deployed in practice.

Appendix 5 Composition of the supervisory committee

Chairman	
Prof. mr. dr. M.F.H. (Marianne) Hirsch Ballin	Professor of Criminal Law and Criminal Procedure, VU University Amsterdam
Members	
Mr. K. (Koen) Hermans	National cybercrime officer, Public Prosecution Service
Lec. dr. J. (Jurjen) Jansen	Lecturer Digital Resilience, NHL Stenden
Dr. mr. D.A.G. (Dave) van Toor	Assistant Professor of Criminal (Procedural) Law, Utrecht University
Mr. M. (Madiha) Malik	Policy advisor DGPenV, Ministry of Justice and Security

The WODC (Research and Documentation Centre) is the knowledge centre in the field of the Dutch Ministry of Justice and Security. The WODC carries out independent scientific research for policy and implementation purposes; it does so both by itself, and on the WODC's commission.

More information:

www.wodc.nl